INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS SERVICES AGREEMENT

Between

County of San Diego

and

Peraton Enterprise Solutions LLC

Contract 568996

November 15, 2016

And as Amended and Restated

On July16, 2019 (version 01)

On February 1, 2023 (version 02)

On November 15, 2024 (version 03)

Contents

List of Schedules, Exhibits, and Appendices viii
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS SERVICES AGREEMENT 1
PART I – PURPOSE AND SCOPE 1
1. Purpose and Scope 1
1.1. Background and Purpose 1
1.2. Requirements; Engagement 2
1.3. Improvement of Government 2
PART II – TRANSITION OBLIGATIONS 3
2. Transition 3
2.1. Transition Services 3
2.2. Milestones for Transition 4
2.3. Progress Reports 4
2.4. Early Access by Contractor 4
2.5. Cutover 4
3. Transition of Assets, Leases, Contracts and Personnel 5
3.1. Transition of Responsibilities for Retained Assets 5
3.2. Reserved 5
3.3. Asset Purchase 5
3.4. Interim Assets 5
3.5. Assignment of Leases and Contracts 6
3.6. Required Consents 6
3.7. Human Resources 7
PART III – SCOPE OF SERVICES 7
4. Services 7
4.1. Scope 7
4.2. General Description of Services 7
4.3. Operational Services 8
4.4. Asset Management 8
4.5. Current Projects 9
4.6. Service Compatibility 9
4.7. RESERVED 10
4.8. Service Levels 10
4.9. Root Cause Analysis and Resolution 11
4.10. Non-Exclusivity 12
4.11. Location of Performance 13
4.12. Critical Milestones 13
4.13. Value Added Services – San Diego Futures Foundation 13

5. Reporting 14
5.1. General 14
5.2. Media 14
6. Disentanglement 14
6.1. General Obligations 14
6.2. Disentanglement Process 15
6.3. Specific Obligations 15
6.4. Preparation for Disentanglement 18
PART IV - CONTRACT ADMINISTRATION 20
7. Administrative Obligations 20
7.1. Viruses and Disabling Devices 20
7.2. End-User Satisfaction and Communication Plan 20
7.3. Standards and Procedures Manual 20
7.4. Contractor Responsibilities for Assets 21
7.5. Retained Assets Managed by Contractor 21
7.6. Dedicated Resources 22
8. Provision of Resources by the County 23
8.1. Office Space and Furnishings 23
8.2. Specific Hardware and Carrier Charges 23
8.3. Access to Personnel and Information 23
8.4. Other Facility and Location Related Obligations 23
9. County-Retained Authority 25
9.1. Strategic and Operational Planning 25
9.2. Service Design and Delivery 26
9.3. Installations, Moves, Adds, and Removes 26
9.4. Applications Development 26
9.5. Business Process Reengineering 26
9.6. Contract Management 26
9.7. Budget Management 27
9.8. Validation and Verification 27
9.9. Other Retained Authority 27
9.10. Review and Acceptance 27
10. RELATIONSHIP MANAGEMENT 30
10.1. Personnel 30
10.2. Replacement of Personnel 32
10.3. Relationship Management 32
10.4. Parties' Relationship 32
10.5. Extraordinary Events or Circumstances 32
10.6. Executive Meetings; Status Meetings 33
10.7. Limitation of Future Contracts 33
10.8. Notice of Adverse Impact 33

11. Service Request Procedures; Change Management Procedure 33
12. Security and Protection of Information 34
12.1. Security 34
12.2. Protection of County Confidential Information 36
12.3. Protection of Public Record Data 37
12.4. Legally Required Disclosure 38
12.5. Notification 38
12.6. Injunctive Relief 38
12.7. Return of County Confidential Information 39
12.8. Confidentiality Agreements and Training 39
12.9. Statutory Requirements Prevail 39
12.10. Contractor Confidential Information 39
13. Recordkeeping and Audit Rights 40
13.1. Recordkeeping 40
13.2. Operational Audit Rights 40
14. Use of Affiliates and Subcontractors 41
14.1. Approval; Key Subcontractors 41
14.2. Subcontractor Agreements 41
14.3. Liability and Replacement 42
14.4. Subcontractor Liability 42
14.5. Direct Agreements 42
15. Proprietary Rights 42
15.1. County Works 42
15.2. Contractor Works 43
15.3. Work Product 43
15.4. Third-Party Works 45
15.5. Residuals 45
15.6. No Limitation of Governmental Rights 45
15.7. Rights and Licenses 45
15.8. County Data 46
15.9. Cooperation 47
PART V – PRICING 47
16. Financial Terms 47
16.1. Fees 47
16.2. Invoices 48
16.3. Pricing Audit 48
16.4. Reduction of Payments 49
16.5. Taxes 49
16.6. Creation of Possessory Interest 49
16.7. Benchmarking 50
16.8. Fee Adjustments 50

16.9. Only Payments 50
16.10. Set-Off 50
16.11. Disputed Amounts 51
16.12. Most-Favored Customer 51
16.13. RESERVED 51
16.14. Capital Infusion and Depreciation 51
PART VI-GENERAL 52
17. Term 52
17.1. Initial Term; Renewals 52
17.2. Early Termination 53
17.3. Termination for Default 54
17.4. Termination for Force Majeure Event 54
17.5. Termination by the County 54
17.6. Effect of Ending of Term 55
17.7. No Termination by Contractor 55
18. Remedies; Limitations of Liability 55
18.1. Remedies Cumulative 55
18.2. Limitation of Liability and Disclaimers 55
18.3. Force Majeure Events 57
19. Insurance 58
20. Legal Compliance 58
20.1. Compliance with All Laws and Regulations 58
20.2. Contractor Permits and License 58
20.3. Americans with Disabilities Act 58
20.4. Equal Opportunity 59
20.5. Non-Discrimination 59
20.6. AIDS Discrimination 59
20.7. Contractor Certification 59
20.8. Board of Supervisors' Policies 59
20.9. Debarment and Suspension 59
20.10. Hazardous Materials 60
20.11. Prohibited Contracts 60
20.12. Political Activities Prohibited 61
20.13. Lobbying 61
20.14. Religious Activity Prohibited 61
20.15. Drug and Alcohol-Free Workplace 61
20.16. Cartwright Act 62
20.17. Zero Tolerance for Fraudulent Conduct In County Services 62
20.18. Family-Centered Practice, Board of Supervisors Policy E-13 62
20.19. Interlocking Directorate 62

20.20. Zero Tolerance in Coaching Medi-Cal or Welfare Clients (Including Undocumented Immigrants) ... 62
20.21. Equal Employment Opportunity ... 63
20.22. Contracting With Small and Minority Businesses, Women's Business Enterprises, and Labor Surplus Area Firms ... 65
20.23. Davis-Bacon Act ... 66
20.24. Copeland Anti-Kickback Act ... 66
20.25. Contract Work Hours and Safety Standards Act ... 66
20.26. Clean Air Act and the Federal Water Pollution Control Act ... 67
20.27. Debarment and Suspension ... 68
20.28. Byrd Anti-Lobbying Amendment ... 68
20.29. Procurement of Recovered Materials ... 69
20.30. Access to Records ... 70
20.31. Rights to Inventions Made Under a Contract or Agreement ... 70
20.32. DHS Seal, Logo, and Flags ... 70
20.33. Compliance With Federal Law, Regulations, and Executive Orders ... 70
20.34. No Obligation By Federal Government ... 70
20.35. Program Fraud and False or Fraudulent Statements or Related Acts ... 71
20.36. Domestic Preferences ... 71
20.37. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment ... 71
21. Representations and Warranties ... 72
21.1. Contractor Representations, Warranties, and Related Covenants ... 72
21.2. County's Representations, Warranties, and Covenants ... 76
21.3. Warranty Disclaimer ... 76
21.4. Waiver ... 76
22. Indemnification ... 76
22.1. Technology ... 76
22.2. Injury, Property, or Other Damage ... 77
22.3. ThirdParty Contracts ... 77
22.4. Misrepresentation ... 77
22.5. Transitioned Employees ... 78
22.6. Hazardous Material ... 78
22.7. Proprietary Information Disclosure ... 78
22.8. General Obligation ... 78
23. Dispute Resolution ... 79
23.1. Procedures To Be Established ... 79
23.2. De Minimis Disputes ... 79
23.3. No Termination or Suspension of Services ... 80
23.4. No Limitation on County Remedies for Default ... 80
24. Other Miscellaneous ... 80
24.1. Entire Agreement ... 80

24.2. Order of Precedence 80
24.3. Conflicts, Errors, Omissions, and Discrepancies 81
24.4. Updates 81
24.5. Captions; References; Terminology 81
24.6. Assignment 82
24.7. Notices to a Party 82
24.8. Amendments; Waivers 83
24.9. Relationship Between, and Legal Status of, the Parties 84
24.10. Severability 84
24.11. Counterparts 84
24.12. Laws and Regulations 84
24.13. County Approval of Promotions 84
24.14. Venue and Jurisdiction 85
24.15. Governmental Immunity 85
24.16. No ThirdParty Beneficiaries 85
24.17. Expenses 85
24.18. Survival 85
24.19. Neither Party Considered Drafter 85
24.20. NonSolicitation 85
24.21. Reserved 86

List of Schedules, Exhibits, and Appendices

Schedule A	Definitions
Appendix A.2	*Assigned Contracts*
Appendix A.3	*Assigned Leases*
Appendix A.4	*Contractor Software*
Schedule 1.2	Offerror's Proposal
Schedule 2.1	Transition Plan
Schedule 2.2	Termination Fees During Transition
Schedule 3.2	Form Bill of Sale
Schedule 3.3	Form Assignment and Assumption Agreement
Schedule 4.3	Operational Services
Appendix 4.3-1	*Contractor's Solution*
Appendix 4.3-2	*Audio / Video Configuration and Support*
Schedule 4.4	Asset Management Upgrades and Enhancements
Schedule 4.8	Service Levels
Exhibit 4.8-1	*Special Service Level Requirement*
Schedule 5	Invoices and Reports
Exhibit 5.1	*Telecom Fees*
Schedule 7.2	End-User Satisfaction Surveys
Schedule 7.3.1	Standards and Procedures Manual Topics List
Schedule 7.6	Shared Resources
Schedule 8.1	License Agreement
Schedule 10.1.1	Contractor Key Personnel
Schedule 10.3	Relationship Management
Schedule 12.1.1	Information Privacy and Security, Criminal Offender Record Information, California Law Enforcement Telecommunication Systems, and County Facility Access
Exhibit 12.1.1-1	*County Privacy Incident Report Form*
Exhibit 12.1.1-2	*CORI-CLETS Training Request Form*

Exhibit 12.1.1-3	*Employee-Volunteer Statement Form*
Exhibit 12.1.1-4	*Private Management Control Agreement*
Exhibit 12.1.1-5	*Federal Bureau of Investigations Criminal Justice Information Services Security Addendum*
Schedule 14.1	Approved Subcontractors
Schedule 16.1	Fees
Exhibit 16.1-1	*Resource Unit Price Summary*
Exhibit 16.1-1a	*Fees Sample Calculation*
Exhibit 16.1-1 Appendix 1	*New Site Install Variable Components*
Exhibit 16.1-2	*Resource Unit Price Decomposition*
Exhibit 16.1-3	*Maximum Annual Fee*
Exhibit 16.1-4	*Labor Categories*
Exhibit 16.1-5	*Firm Fixed Price for Applications M&O*
Exhibit 16.1-5b	*Firm Fixed Price for Applications M&O*
Exhibit 16.1-6	*Resource Unit Price Summary Option Term*
Exhibit 16.1-6a	*Resource Unit Price Decomposition Option Term*
Exhibit 16.1-7	*ELA Pricing Adjustments*
Schedule 16.7	Benchmarking Methodology
Schedule 16.8	Fee Reductions
Schedule 18.2	Third Party Contracts
Schedule 19	Insurance

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS SERVICES AGREEMENT

This Information Technology and Telecommunications Services Agreement ("Agreement"), dated as of November 15, 2016 (the "Signing Date"), is a contract between the County of San Diego (the "County"), acting through its Chief Administrative Officer and Purchasing Agent, having offices at 5560 Overland Avenue, Suite 270, San Diego, California 92123-1204, and Peraton Enterprise Services LLC ("Contractor"), a Limited Liability Company having offices at Herdon, VA (together, "the parties" or "the Parties"), under which Contractor shall provide the County with certain information technology ("IT") and telecommunications services, on the terms and conditions set forth below. Capitalized terms used herein, if not defined, shall have the meanings assigned to them in Schedule A.

For and in consideration of the mutual promises and covenants contained herein, the receipt, sufficiency, and adequacy of which are hereby acknowledged, the Parties, intending to be legally bound, hereby contract and agree as follows:

PART I – PURPOSE AND SCOPE

1. Purpose and Scope

1.1. Background and Purpose

The County has undertaken a comprehensive outsourcing initiative, the primary goal of which is to continuously improve the County's use of IT and telecommunications and the manner in which the County receives its IT and telecommunications Services. The Services provided by Contractor under this Agreement will allow the constituents of the County to benefit from the enormous potential of IT and telecommunications, as applied to the business of government. In addition, the Contractor-provided IT and telecommunications Services will be provided by Contractor in a manner that will allow the County to be more efficient in the business of government and in its provision of services to the constituents of the County. The Contractor provided IT and telecommunication Services will also support the County in its activities to create economic opportunities for the constituents of the County.

Another primary purpose of this Agreement is for the County to receive, through Contractor, IT and telecommunications Services that provide continuous state-of-the-art security systems and methods that will ensure the privacy and protection of the County's Confidential Information and data. These Services, and Contractor's obligations related thereto, are described in more detail in Sections 12, 15, and Schedules 12.1.1 and 4.3. In addition to being bound by this Agreement to perform these specific tasks within the timelines contained herein, Contractor will at all times be fully subject to and bound to comply with all applicable County, State, and federal laws, rules, and regulations relating to the subject matter hereof, including those regarding privacy and the protection of the County's Confidential Information and data.

This Agreement becomes effective on its Signing Date, subject to the Board of Supervisors authorizing the Director of the Department of Purchasing and Contracting to award the Agreement to Contractor. Only after these County and all applicable State and federal approvals are obtained will this Agreement become effective. Concurrently with these review periods, Contractor is expected to continue working with the County and the Legacy Provider to complete all tasks

necessary to prepare for a smooth cutover of operational responsibility for the IT and telecommunications Services described herein. As of the Cutover Date for each Service Framework, Contractor will assume such operational responsibility by becoming the employer or causing one of its subcontractors to become the employer of all Designated Employees and any other employees transitioned from the Legacy Provider under such Service Framework.

1.2. Requirements; Engagement

The County has described its requirements for IT and telecommunications Services in the County's Request for Proposals dated February 8, 2016, including questions from potential proposers and County responses to those questions (collectively the "RFP") and other requests and communications. In response to the RFP, Contractor has delivered to the County various documents and other communications, as described in Schedule 1.2, and its Best and Final Offer (the "BAFO") (collectively, the "Responses"), in which Contractor represented, among other things, that it could provide IT and telecommunications Services satisfying the RFP. Accordingly, in reliance upon the Responses and in furtherance of the purposes for which the Responses were solicited, the County, under the authority of the Board of Supervisors' action dated November 15, 2016, hereby engages Contractor to perform all of the obligations imposed on it, including the Services, pursuant to this Agreement, and Contractor hereby accepts such engagement and promises to perform according to this Agreement. Contractor shall be the prime contractor and hereby assumes full and total responsibility for providing all of the Services and for obtaining all Assets, documentation, services, and other resources that it will need in order for it to be able to provide the Services.

1.3. Improvement of Government

The general goal of the County under this Agreement is for Contractor to provide to County and for County to receive continuously improving IT and telecommunications Services. This Agreement shall improve the County's capabilities to serve its constituents, reduce County's operating costs and facilitate constituents' access to the services the County and its related entities furnish, among other benefits. The Services shall allow the constituents of the County to continue to benefit from the enormous potential of IT and telecommunications, as applied to the business of government. The objectives of the County under this Agreement include the following:

(a) Providing the most efficient processing of and access to information, which will reduce wait times at County facilities;

(b) Eliminating the need to visit multiple County offices through the use of integrated systems and business processes that promote "one-stop shopping";

(c) Continuously improving delivery of public services and the County's central system and information infrastructure;

(d) Promoting private enterprise through electronic commerce, enabling businesses to submit plans and other documents for County approval without the labor and expense of paper submittals;

(e) Reducing the number of trips that constituents must take to transact business with divisions of County government;

(f) Improving Internet access to County resources;

(g) Helping ensure that tax dollars are used efficiently and not wasted on obsolete, inefficient systems and business processes;

(h) Providing the highest levels of customer service;

(i) Increasing public access to County services by providing reliable communications and an information infrastructure with multiple points;

(j) Saving the County and its customers time by providing service alternatives to visiting County facilities;

(k) Increasing responsiveness to commercial requests for information and services;

(l) Allowing managers to focus on improved business processes that reduce the cost of government and permit the County's Board of Supervisors to allocate savings for reinvestment in new or existing programs;

(m) Allowing the County to focus on its core competencies and business priorities;

(n) Providing timely information for executive decision-making through maintaining state-of-the-art enterprise-wide systems for financial accounting, payroll, procurement, and human resources;

(o) Augmenting the County's capabilities in financial planning and monitoring;

(p) Increasing the County's pool of technology resources and capabilities;

(q) Providing reliable, efficient computing systems and voice telecommunications to support job functions;

(r) Minimizing labor-intensive tasks that do not add commensurate value;

(s) Providing decision-support tools to workers;

(t) Providing state-of-the-art computing tools and training to enhance career development; and

(u) Providing comprehensive Asset management and control.

For each of the above-described objectives, as well as for Contractor's other obligations under this Agreement, Contractor shall continuously improve upon the Services it provides to County while reducing overall cost to the County for the Contractor to provide the Services.

PART II – TRANSITION OBLIGATIONS

2. Transition

2.1. Transition Services

Contractor shall accomplish the transparent, seamless, orderly, and uninterrupted transition from the manner in which the County currently receives all Current Services to the provision of all of such services, and all other Services, to the County by Contractor (the "Transition"). Such Transition shall include the complete and timely performance by Contractor of all requirements set forth in the Transition Plan, attached as Schedule 2.1, in accordance with the due dates specified

therein and shall be accomplished by Contractor in such a manner as to have no adverse effect upon the County, any agency, subdivision or department thereof, nor upon the quality or continuity of the IT and telecommunications services being provided to such entities. From and after the opening of business on the Cutover Date of the first Service Framework transitioned to Contractor, Contractor shall ensure that there is no material adverse effect on the quality of the IT and telecommunications-related Services provided to the County and to the End-Users, that would not have otherwise occurred had the Transition contemplated by this Agreement not taken place.

2.2. Milestones for Transition

The Parties recognize and agree that time is of the essence for a successful Transition and they have designated certain actions and projects in the Transition Plan as Transition Milestones. If Contractor fails to meet any such Transition Milestone by the date corresponding thereto in the Transition Plan, Contractor shall be subject to Fee Reductions pursuant to Section 16.8 hereof. In the event that Contractor anticipates that action or inaction by the County could impact a Transition Milestone, Contractor may request an extenstion on such Transition Milestone, approval of which shall not be unreasonably withheld by the County. Should the County Terminate for Convenience during the transition, the County shall pay the terminations fees as set forth in Schedule 2.2, Termination Fees During Transition. Any such termination fee due to Contractor shall be reduced by any Transition Milestone payment that has been made to Contractor by County. Notwithstanding the foregoing, the County may remove, at its discretion, the work described in Section 2.18 of Appendix 4.3-1, Contractor's Solution, prior to Contractor performing that work and any such future termination fee shall be reduced by the value of this removed work. Notwithstanding the foregoing, if Contractor fails to complete the transition of all Services to Contractor by October 10, 2017, the County may terminate this Agreement for cause without requirement of notice or opportunity for cure.

2.3. Progress Reports

Contractor shall provide to the CIO a written update as to progress of the Transition Plan at least weekly until such plan and each of Contractor's responsibilities thereunder have been met.

2.4. Early Access by Contractor

During the period between the Signing Date and the final Cutover Date for the last Service Framework transitioned to Contractor, the County shall (and shall use reasonable efforts to cause the Legacy Provider to) provide Contractor with reasonable access to the Retained Assets, the Purchased Assets, and the Designated Employees, but solely for the purpose of reasonably assisting and cooperating with Contractor in the accomplishment of the Transition in accordance with the Transition Plan, and only to the extent that Contractor is required to have access to such resources (as distinct from other resources that Contractor may then have or could procure) in order to accomplish the Transition in accordance with the Transition Plan.

2.5. Cutover

In the event that the County determines, in its sole discretion, at any time during the Transition, that the County, the End Users, any agency, department or subdivision of the County or the quality or continuity of the Services has been materially and adversely affected in any way, or that any such material and adverse effect seems reasonably likely to occur, then the County shall direct Contractor

to stop and proceed no further with such transition or portion thereof until such time as Contractor shall have: (i) analyzed the cause of such effect; (ii) developed a reasonable plan for resuming such transition in such a manner as to eliminate or avoid such effect (and any other negative or adverse consequences of such transition; and (iii) received the County's approval to proceed with such Transition, which approval shall not be unreasonably withheld. Following any resumption of the transition of the Services to Contractor, if the County again determines that a material and adverse effect has occurred, then the process described above in this Section 2.5 shall be repeated. Nothing in this Section 2.5, nor the County's exercise of its rights, as described above, pursuant to this Section 2.5, shall in any way reduce, limit, or obviate any obligation of Contractor to meet a Transition Milestone or any other schedule, target, completion schedule, or other commitment specified in the Transition Plan or this Agreement. In addition, the County's exercise of its rights as set forth in this Section 2.5 shall not trigger any additional charges or fees from the Contractor.

3. Transition of Assets, Leases, Contracts and Personnel

3.1. Transition of Responsibilities for Retained Assets

On each Cutover Date, and from and after each such date, Contractor shall assume responsibility for the administration and management of the Retained Assets pertaining to the applicable Service Framework in accordance with Section 7.5 and Schedule 4.3.

3.2. Reserved

3.3. Asset Purchase

As of each Cutover Date, the County or its Legacy Provider (as applicable) shall sell at Net Book Value to Contractor, and Contractor shall buy from the County or its Legacy Provider (as applicable), "AS IS, WHERE IS" and without any express or implied warranties of any kind, all of the County's (or the Legacy Provider's) right, title, and interest in and to the Purchased Assets. The Parties will enter into Bills of Sale relating to Contractor's purchase of the Purchased Assets in the form attached hereto as Schedule 3.2 and dated as of each Cutover Date. The Net Book Value of the Purchased Assets is set forth on Schedule 2.2 attached hereto.

3.4. Interim Assets

The Parties acknowledge that during the period between the Signing Date and each Cutover Date pertaining to a Service Framework, the County (and Legacy Provider) will acquire additional assets that may be useful for Contractor's use in performing the Services under an applicable Service Framework ("Interim Assets") and during such period the County (and Legacy Provider) will advise Contractor of all pertinent information with respect to all Interim Assets. For a ninety (90) day period commencing on each Cutover Date, Contractor shall have the right to use and the option to purchase whichever of the Interim Assets applicable to the Service Framework cut over on such Cutover Date that it may elect to use or purchase. If Contractor elects to use an Interim Asset during such ninety (90) day period to provide the Services, such Interim Asset shall be deemed to be a Retained Asset until the earliest of: (i) ninety (90) days after the applicable Cutover Date; (ii) the date that Contractor specifies to the County (or Legacy Provider) as the date on which it will no longer use such Interim Asset; and (iii) the date on which Contractor purchases such Interim Asset as provided herein. Contractor will have the option, exercisable from time to time within ninety (90) days of such Cutover Date, to purchase at its then Net Book Value any Interim Asset that it is

using to provide the Services, as mutually agreed by Contractor and the County (or the Legacy Provider, as applicable). An Interim Asset purchased by Contractor pursuant to this Section 3.4 will thereafter be deemed to be a Purchased Asset.

3.5. Assignment of Leases and Contracts

Subject to Contractor obtaining any Required Consents, the Parties (and/or Legacy Provider) shall enter into Assignment and Assumption Agreements in the form attached hereto as Schedule 3.5 pursuant to which the County (and/or Legacy Provider), as of the applicable Cutover Date, shall assign to Contractor all of the County's (or Legacy Provider's, as applicable) rights under the Assigned Leases and the Assigned Contracts pertaining to the Service Framework corresponding to such Cutover Date. Contractor shall assume responsibility for, and shall perform, all obligations of the County (and Legacy Provider) under the Assigned Leases and Assigned Contracts, including payment of all related expenses (including maintenance fees), to be performed with respect to periods on or after each such Cutover Date, and shall indemnify the County and Legacy Provider with respect to all such obligations. Contractor shall be responsible for paying all relicensing and transfer fees associated with the Assigned Leases and Assigned Contracts. Contractor shall reimburse the County for any prepayments in respect thereof (provided that, all "prepayments", as such term is used in this Agreement, shall be for goods or services of which Contractor receives the benefit after the applicable Cutover Date and that will be utilized on or after the applicable Cutover Date in connection with the performance of Services by Contractor hereunder, including, for example, prepaid support and maintenance service fees), and Contractor shall indemnify the County and Legacy Provider (as applicable) with respect to all such obligations in respect of such periods. The County or its Legacy Provider (as applicable) shall be responsible for the performance of all obligations of the County under the Assigned Leases and Assigned Contracts, including payment of all related expenses, to be performed with respect to periods prior to the applicable Cutover Date, and shall indemnify Contractor with respect to all such obligations in respect of such periods. From time to time, to the extent permitted by the applicable agreement, Contractor may request that the County cooperate in the termination of any Assigned Leases or Assigned Contracts (which cooperation shall not be unreasonably withheld by the County), and Contractor shall reimburse the County or its Legacy Provider (as applicable) for all termination charges or penalties, if any.

3.6. Required Consents

With the County's cooperation, Contractor shall obtain all Required Consents. In the event that Contractor is not able to obtain any Required Consent despite the use of its best efforts, then, unless and until such Required Consent is otherwise obtained, the Parties shall cooperate with each other and the Legacy Provider in achieving a reasonable alternative arrangement under which Contractor may perform the Services without causing a breach or violation of any agreement for which a Required Consent is to be obtained. Such reasonable alternative arrangements may include: (i) Contractor obtaining such consent to Contractor's use of the relevant Assets as the relevant party will agree to provide; or (ii) Contractor procuring a suitable replacement for the Assets for which it is unable to obtain the Required Consent. Contractor shall be responsible for paying all termination fees associated with any agreement for which Contractor is unable to obtain a Required Consent. All obligations under this Section 3.6 shall be the responsibility of Contractor, at its cost and expense, except in the following regards: (A) each Party shall take such actions, at its own

cost and expense, as are required of it by applicable laws or regulations with respect to the Government Approvals; and (B) the County shall obtain, at its cost and expense, all Required Consents for contracts for Retained Assets entered into by the County after the Cutover Date applicable to the Service Framework for which the County entered into such contracts. The County reserves the right to reasonably request and review any or all such Required Consents prior to the commencement of any Services hereunder.

3.7. Human Resources

Contractor shall offer employment with Contractor, or shall cause one of its Subcontractors to offer employment with such Subcontractor, effective on the applicable Cutover Date, to all Designated Employees. In addition, prior to the applicable Cutover Date, Contractor shall make such offers of employment as are necessary in order for Contractor to provide all applicable Services on and after the applicable Cutover Date.

PART III – SCOPE OF SERVICES

4. Services

4.1. Scope

In accordance with this Agreement, Contractor shall fulfill all of the IT and telecommunications Services requirements of the County at all times during the Term (subject to the provisions of Section 4.10). The scope of the County's IT and telecommunications requirements consists of the performance of the Services. Although the Parties have attempted in this Section 4 and the associated Schedules to delineate the specific Services to be provided by Contractor, the Parties acknowledge that some items may not have been specifically identified herein. The specific enumeration in any particular Section of this Agreement of certain of Contractor's duties or obligations is not an implied limitation on, or alteration of, other duties or obligations imposed on Contractor elsewhere in this Agreement. In the event of any dispute between the Parties as to whether a particular service or function falls within the scope of the Services to be provided by the County's Third-Party service providers, or by the County itself, or within the scope of those to be provided by Contractor, such particular service or function shall be considered to be a part of the Services hereunder if it is consistent with, and reasonably inferable to be within, the scope of the Services hereunder and it more reasonably would be associated with the Services than with the scope of the services to be provided by such other service providers.

4.2. General Description of Services

Subject at all times to the County's exercise of its management and oversight functions and prerogatives, as identified in Section 9 or otherwise, and subject to the provisions of Section 4.10 hereof, Contractor shall perform all of the Services, and shall operate in the capacity of the County's IT and telecommunications department, and shall do everything that is required to provide the entire IT and telecommunications function to the County. In all cases, Contractor shall deliver high-quality, continuously improving, value-added Services that assist the County in effectively utilizing IT and telecommunications to enhance the quality and value of the County's services to its constituents. If not otherwise provided in this Agreement, with respect to any tasks, functions, and services that are within the scope of Services but with regard to which there is no set or fixed timetable or schedule for performance and which are therefore to be provided upon the County's

request, Contractor shall promptly perform such Services. Contractor shall at all times use all commercially reasonable efforts (which, at a minimum, shall be consistent with best industry standards and practices) to avoid, prevent, and mitigate any material adverse effect on the continuity and quality of the Services being provided to the County. Except as expressly set forth in this Agreement, Contractor shall furnish all labor, materials, equipment, products, tools, transportation, and supplies required to perform the Services.

4.3. Operational Services

4.3.1. Performance of Services

Commencing at 12:00:00 a.m., local time, on each Cutover Date, and at all times thereafter during the Term, except as otherwise expressly stated herein, and subject to the qualifications, limitations, and exclusions expressed elsewhere in this Agreement (including any exceptions expressed in the Transition Plan or in Schedule 4.3), Contractor shall perform, at all Locations, all Current Services for the applicable Service Framework and all of the Services described in Schedule 4.3 for the applicable Service Framework.

4.3.2. Procurement

Subject to the approval of the County, Contractor shall, as necessary to perform the Services, procure all Assets; evaluate Subcontractor and Third Party qualifications and independence; negotiate prices; obtain the most favorable rates and discounts available; distribute and install all procured Assets; and ensure Software and Hardware license compliance. All procurement activities necessary for Contractor to provide the Services, and all purchase prices, license fees, lease payments, and support and maintenance fees for all procured Assets, shall be paid for by Contractor.

4.3.3. OIC Procurement of Additional Resources

In accordance with Section 4.8 of Schedule 4.3, Contractor shall also procure Assets as the Contracting Officer might direct it to make, at the lowest available prices. Contractor and the County shall coordinate procurements in order to obtain benefits from volume purchases and to promote compatibility of IT and telecommunications Assets throughout the County. All procurements shall be from the County's lists of approved manufacturers of Hardware and Software and shall be owned (or for COTS Software, licensed) by the County free and clear, without any liens or encumbrances, unless otherwise agreed in writing by the County in its sole discretion.

4.4. Asset Management

4.4.1. Asset Management: Upgrades, Enhancements and Replacements

Contractor shall provide the Asset management and upgrade services described in Schedule 4.3 and Schedule 4.4 throughout the Term. Unless otherwise directed by the County, such Services shall include procurement, installation, implementation, integration and maintenance of upgraded and replacement Assets and enhancements to Assets for all Purchased Assets and all other Assets, excluding Retained Assets, used in the provision of Services, in accordance with such Schedules. In fulfilling its obligation to perform all services to procure, install, implement, integrate and maintain upgrades, enhancements and

replacements hereunder, Contractor shall provide the County with Assets that meet the then-current standards and specifications for each such Asset in the Standards and Procedures Manual, Schedule 4.3 and Schedule 4.4 or as otherwise agreed to in writing by the Parties. Contractor shall also procure, install, implement and integrate enhancements and replacements and provide maintenance services at no additional cost to the County and shall schedule such upgrades, enhancements, replacements, integration and maintenance services in advance and in such a way as to prevent any interruption or disruption of Services to the County. Contractor shall obtain the prior written consent of the County before procuring, installing, implementing, integrating, maintaining, upgrading, enhancing or replacing any Asset that is used or to be used by the County, Contractor, or Third Parties in connection with the provision of the Services if such procurement, installation, implementation, integration, maintenance, upgrade, replacement, or enhancement could result in any additional cost to the County hereunder or any diminution in the nature or level of any portion of the Services.

4.4.2. Continuous Improvement

Contractor and County acknowledge that technology and the provision of IT and telecommunication Services must continuously improve. As part of Contractor's obligation to continuously improve the Services, Contractor shall annually, and no later than September 30th of each year, provide to County a report on what improvements Contractor has made since its previous report and what improvements it intends to make in the next year. These activities may include, but are not limited to, technology and the way the Services are provided so that the County's costs will decrease, and Contractor will increase the efficiency and timeliness of the provision of Services to County and County's provision of services to its constituents, and/or improve the quality of Services provided to County or that County provides to its constituents. Contractor shall provide the report by Service Framework.

4.5. Current Projects

Contractor shall provide the continuing and uninterrupted development and implementation of all Current Projects and shall conduct such development and implementation in accordance with the then-current written plans for such Current Projects, if such plans exist, or if no such written plans exist, as such Current Projects are being performed as of the Cutover Date applicable to the Service Framework for which such Current Projects are being performed. Contractor shall provide to County, or if the Legacy Provider has an Agreement with a Third-Party who has contracted with the County that Third-Party, the continuing and uninterrupted development and implementation of all Current Projects for the lessor cost of i) the then-current projected budget, including resource units and hourly rates, ii) the existing agreed-to fixed price, or iii) Contractors resource unit and hourly rates for Services.

4.6. Service Compatibility

Contractor shall ensure that all Assets utilized by Contractor or approved by Contractor for utilization by the County in connection with the Services shall be successfully integrated and interfaced, and shall be compatible, with all other Assets that are being provided to, recommended to, or approved for use by, the County by Third-Parties or the County itself. Further, Contractor

shall ensure that none of the Services or other items provided to the County by Contractor shall be adversely affected by, or shall adversely affect, those of any such Third-Party or the County, whether as to functionality, speed, SLs, interconnectivity, reliability, availability, performance, response times, or similar measures. To the extent that any interfaces need to be developed or modified in order for the Assets to integrate successfully, and be compatible, with the Third-Party Assets, Contractor shall develop or modify such interfaces as part of the Services, pursuant to a Service Request in accordance with the process set forth in Section 11. In the event of any dispute as to whether a particular defect, malfunction, or other difficulty was caused by products or services furnished by Contractor or by products or services furnished by any provider of the Third-Party Assets, Contractor shall be responsible for correcting at its cost, such defect, malfunction, or difficulty, except to the extent that Contractor can demonstrate, to the County's satisfaction, by means of a Root-Cause Analysis, that the cause was not a product or service furnished by Contractor. In addition, Contractor agrees that at all times during the Term it shall cooperate with Third-Parties to coordinate its provision of the Services with the services and systems of such Third-Parties. Such cooperation and access shall include: (i) facilitating with such other relevant Third-Parties the prompt and timely resolution of all problems that may arise and impact the Services or the respective use, operation, support, maintenance, or provision thereof, regardless of the actual or suspected root cause of such problems, and using all commercially reasonable efforts to obtain and maintain the active participation, cooperation, and involvement of such other Third Parties as is required for such problem-resolution; (ii) providing applicable written information concerning any or all of the systems, data, computing environment, and technology direction used in providing the Services; (iii) working with the Third-Parties in the integration of the Services with the Assets in the County's environment and, as reasonably requested, the integration and interfacing of the Assets of such Third-Parties with the Services as well as providing reasonable assistance and support services to such Third-Parties; (iv) providing access to Contractor and County systems and architecture configurations to the extent reasonably required for the activities of such Third-Parties; and (iv) providing access to and use of the Assets. If any of the foregoing require the disclosure of any Contractor Confidential Information to any Third-Party, such Third-Party shall enter into a confidentiality agreement, with terms at least as restrictive as those in this Agreement with the County.

4.7. RESERVED

4.8. Service Levels

4.8.1. Commitment to SLs

Except as otherwise specified in this Agreement, Contractor shall perform all Services at least in accordance with the SLs. The SLs are set forth in Schedule 4.8. Certain terms and definitions applicable to the SLs of Schedule 4.8 are specified in Schedule A. All Assets provided, maintained or developed by Contractor pursuant to the terms hereof shall incorporate methods permitting measurement of performance-related SLs.

4.8.2. SL Measurement and Reporting

Contractor shall at its own expense measure and report its performance against the SLs, including measurement and reporting for the County, during each month by the fifteenth (15th) day (or following business day if such fifteenth (15th) day is a weekend or holiday)

of the following month ("SL Measurement Period"). For continuing Failures that occur in consecutive SL Measurement Periods, Contractor shall report such Failures in the month such Failure commences and for each following month during which such Failure continues. The County shall give Contractor reasonable advance notice of anticipated changes in numbers of End-Users or processing volumes. Contractor's report shall be delivered in accordance with Section 4.13 hereof. Contractor shall meet with the CIO at least quarterly, or more frequently if requested by the CIO, to review Contractor's actual performance against the SLs and shall recommend remedial actions to resolve any performance deficiencies.

4.8.3. Continuous Improvement in SLs

The Parties shall review and discuss the SLs and At Risk Pool from time-to-time, but not more frequently than every six (6) months and at least once per year. During each review, in accordance with the SL continuous improvement methodology in Schedule 4.3 and at no additional cost to the County, the Parties shall negotiate increases to the SLs as part of Contractor's obligation to continuously improve the Services. If County and Contractor are unable to agree to an increase in an SL, the County may initiate the Dispute Resolution process.

The SLs exist for the benefit of the County, to reflect (i) improved performance requirements based upon advances in available technology and methods that are suitable for use in performing the Services, (ii) the increased capabilities of any Hardware or Software Contractor acquires to provide the Services, (iii) changes in the operations and environment of the County, and (iv) other changes in circumstances. Contractor shall continuously evaluate ways to improve its performance and the provision of Services to the County, and shall make these improvements available to the County as soon as possible.

4.8.4. Establishing New SLs

The County may, in its sole discretion, establish new SLs. Any newly established SL shall not, without Contractor's agreement, increase the At Risk Pool and shall not be an additional cost to County. The newly established SLs shall be baselined using historical performance levels. After establishing the new SLs and the associated baselines, the County and Contractor shall negotiate targeted improvements for the new SLs. If County and Contractor are unable to agree to the targets, the County may initiate the Dispute Resolution process.

4.8.5. Reallocation of SL At Risk Pool and Increasing the At Risk Pool

The County may, in its sole discretion, reallocate no more often than every six months the weighting of the SL At Risk Pool between existing SLs, and between existing and new SLs. Upon mutual agreement, the SL At Risk Pool may be increased.

4.9. Root Cause Analysis and Resolution

Promptly, and in no event later than five (5) days after Contractor's discovery of, or, if earlier, Contractor's receipt of a notice from the County regarding, (i) as specified in the Standards and Procedures Manual or otherwise as requested by the County, Contractor's failure to provide any of

the Services, (ii) Contractor's failure to meet a Transition Milestone or Critical Milestone, or (iii) any other failure requiring a root-cause analysis as specified in this Agreement, Contractor shall: (A) perform a root-cause analysis to identify the cause of such failure; (B) correct such failure (regardless of whether caused by Contractor); (C) provide the County with a written report detailing the cause of, and procedure for correcting, such failure; and (D) provide the County with satisfactory evidence that such failure will not recur. The correction of any such failure shall be performed entirely at Contractor's expense unless it has been determined, by mutual agreement of the Parties or through any dispute-resolution procedures established by the Parties in writing, that the County (or its subcontractors, agents, or third parties provided by the County and not managed by Contractor) was the predominant contributing cause of the failure and Contractor could not have worked around the failure without expending a material amount of additional time or cost. In such an event, Contractor shall be entitled to temporary relief from its obligation to timely comply with the affected SL or Critical Milestone, but only to the extent and for the duration so affected. For purposes hereof, the preexisting condition of the County's properties and systems shall not be deemed a contributing cause of any failure.

4.10. Non-Exclusivity

4.10.1. Non-Exclusivity

Nothing herein shall prevent the County from obtaining any type of Services, including any discrete component, deliverable, feature, function, capability, task, activities, or portion of the Services, or any other Services, from itself or any other provider during the Term. In this regard, the County may terminate any discrete component, deliverable, feature(s), function(s), capability(ies), task(s), activity(ies), or portion of the Services in accordance with the provisions of Section 17.2.1. In the event the County elects to terminate any such discrete component, deliverable, feature(s), function(s), capability(ies), task(s), activity(ies), or portion of the Services pursuant to the terms hereof, Contractor shall perform its Disentanglement obligations (as described in Section 6) to the extent applicable to the Terminated Services. For clarity, the County shall not be required to terminate any Services pursuant to the provisions of Section 17.2.1 in order to exercise the rights set forth in this Section 4.10.

4.10.2. Cooperation and Coordination

With respect to each Terminated Service, or any other type of Service, including any discrete component, deliverable, feature, function, capability, task, activities, or portion of the Services, or any other services, that the County obtains from itself or any other provider (collectively, "Retained Services"), Contractor shall at all times cooperate and coordinate with the County and the selected provider in every respect to facilitate the successful accomplishment of the Retained Service, provided that such provider complies in all material respects with Contractor's reasonable technical and confidentiality requirements and to the extent that the personnel otherwise assigned to perform the delivery of Services under this Agreement can reasonably do so without materially and adversely affecting the SLs or other aspects of the Services delivered. Such cooperation shall include: (i) providing information concerning any or all of the systems, data, computing environment, and technology direction used in providing the Services; (ii) cooperating with

such Third-Party in the implementation and integration of the Retained Services in the County's environment; (iii) providing access to and use of Contractor resources; and (iv) performing tasks assigned to Contractor in connection with the Retained Services. Contractor acknowledges that the County has the right to solicit or accept proposals on any services within or outside of the scope of the Services from any other provider and may award any service to any such provider for any reason. In no event shall Contractor restrict or otherwise hinder or limit any Subcontractor's ability to perform any services of any kind directly for the County (including the Services described in this Agreement). Contractor acknowledges and agrees that all Subcontractors may communicate directly and without limitation with the County regarding this Agreement, the Services or any other services that may be provided by such Subcontractors directly or pursuant to this Agreement. The obligations described herein shall be in addition to Contractor's Disentanglement obligations as described in Section 6.

4.11. Location of Performance

Except where Contractor obtains the County's prior written approval, Contractor shall perform all of the Services only from or at locations within the United States. Any County approval for the performance of Services outside of the United States shall be limited to the specific instance and scope of such written approval, including the types of Services and locations involved. Notwithstanding the foregoing, this Section 4.11 shall not restrict the country or countries of origin of any assets purchased to provide the Services hereunder; provided, that when such assets are used to provide the Services, such assets shall be used only from or at locations within the geographic boundaries of the continental United States.

4.12. Critical Milestones

From time-to-time during the Term, the County may designate as Critical Milestones certain actions and projects to be completed by the Contractor that are of material importance to the County or the agency, subdivision or department of the County receiving the Services. If Contractor fails to meet any such Critical Milestone by the date agreed by the Parties for such Critical Milestone, Contractor shall be subject to Fee Reductions pursuant to Section 16.8 hereof. In addition, if Contractor fails, or if the County reasonably determines that Contractor is likely to fail, to meet a Critical Milestone by the date agreed by the Parties, then, in addition to any other rights and remedies that may be available to the County in accordance with this Agreement, Contractor shall, at the County's option and at no additional cost to the County, provide such additional personnel as may be required or necessary to accomplish all activities, tasks, and Services that were associated with such Critical Milestone either: (i) as soon as commercially practicable through Contractor's exercise of all commercially reasonable efforts, if Contractor has already failed to meet such Critical Milestone; or (ii) by the date corresponding thereto, as agreed by the Parties at the assignment of Critical Milestone status to a project or action, if such date has not yet passed.

4.13. Value Added Services – San Diego Futures Foundation

During each year of the Term, Contractor shall provide to the San Diego Futures Foundation contributions of $500,000.00 cash. Additionally, for standard personal computers, laptop computers, tablets, and associated peripheral assets owned or leased by the Contractor and that were used by the County, but subsequently permanently retired, decommissioned, or otherwise

removed from service in accordance with Schedule 4.3, Contractor shall, at no additional charge or cost to the County or receiving entity and to the extent such assets still have a remaining useful life, transfer such assets to the San Diego Futures Foundation or any other charitable organization as directed by the CIO or his or her designee.

5. Reporting

5.1. General

Contractor shall furnish the County at no additional charge with reports described in this Agreement in the form, and covering the information, set forth in Schedule 4.13 and with the frequency that the County may request from time-to-time. In addition, from time-to-time, County may identify additional reports arising out of or related to the Services to be generated by Contractor (in the format requested by the County) and delivered to County on an ad hoc or periodic basis. All such reports shall be provided to County as part of the Services and at no additional charge to County. In addition, Contractor shall furnish the County such billing information, in such form, as the County may request in order for the County to be able to administer its chargeback program, as further described in Schedule 4.13. In connection with meeting this obligation, Contractor shall continually maintain (and deliver to County upon request) an up-to-date, accurate list of all assets associated with the Services in such format as may be requested by County in order for it to be able to align the list with the County's chargeback program. Contractor's reports shall also include information regarding: Contractor's performance of the Services; cost-management; Subcontractor relationships; End-User satisfaction; security; and human resources. Contractor shall promptly (but not later than two (2) days after gaining knowledge thereof) inform the County, in writing, of any deficiencies, omissions, or irregularities in the County's requirements or in Contractor's performance of the Services that come to Contractor's attention. Contractor shall furnish the County with all existing and future research and development resources, such as published materials and industry studies conducted for or by Contractor, that come to its attention and pertain to the Services and that might assist the County in setting its IT and telecommunications policies or requirements. Contractor's Account Executive shall also advise the County of all other matters of a material nature, that he or she believes would be helpful to the County in setting or revising its IT and telecommunications policies or requirements.

5.2. Media

Contractor shall furnish the County with all reports in both hard copy and electronic form per the County's specifications as reasonably requested by the County from time to time during the Term.

6. Disentanglement

6.1. General Obligations

Contractor shall accomplish a complete, timely, and seamless transition of any Terminated Services from Contractor and the Subcontractors to the County, or to any replacement provider designated by the County, without any interruption of or adverse impact on the Terminated Services or any other services provided by Third-Parties or Services (and their respective SLs) that Contractor shall continue to provide (each transition, a "Disentanglement"). Contractor shall cooperate with the County and any new service provider and otherwise promptly take all steps required or reasonably requested, to assist the County in effecting a complete and timely Disentanglement of any

Terminated Services. Contractor shall provide all information regarding the Terminated Services or as otherwise needed for Disentanglement, including data conversion, interface specifications, and related professional services. Contractor shall provide for the prompt and orderly conclusion of all Terminated Services, as the County may direct, including completion or partial completion of projects, documentation of work in process, and other measures to assure an orderly transition to the County or the County's designee. Contractor's obligation to provide the Services shall not cease until a Disentanglement satisfactory to the County, including the performance by Contractor of all asset-transfers and other obligations of Contractor provided in this Section 6, has been completed.

6.2. Disentanglement Process

The Disentanglement process shall begin (and the Contractor shall begin the performance of its Disentanglement Services (as defined below) on any of the following dates: (i) the date the County notifies Contractor that no funds or insufficient funds have been appropriated so that the Term shall be terminated pursuant to Section 17.1.1; (ii) the date designated by the County prior to the end of any initial or extended term that the County has not elected to extend pursuant to Section 17.1; or (iii) the date any Termination Notice is delivered, if the County elects to terminate any or all of the Services pursuant to Sections 4.10, 17.2, 17.3, 17.4, or 17.5. Contractor's obligation to perform the Terminated Services, and the County's obligation to pay for the Terminated Services, shall expire: (A) when funds appropriated for payment under this Agreement are exhausted, as provided in Section 17.1.5; (B) at the end of the initial or extended term set forth in Section 17.1; or (C) on the Termination Date, pursuant to Sections 4.10, 17.2, 17.3, 17.4, or 17.5 (with the applicable date on which Contractor's obligation to perform the Terminated Services expires being referred to herein as the "Expiration Date"); provided, however, that Contractor shall remain obligated to provide Disentanglement Services (as defined below) until a Disentanglement satisfactory to the County has been completed, a period that may last up to twelve (12) months after any such Expiration Date. The County shall not pay any additional fees for Disentanglement Services (as defined below) performed by Contractor. In the event the County elects hereunder to terminate a Service Framework, or a component, task, feature, portion, capability, or sub-element of the Services (but not all Services in the aggregate), Contractor shall perform the Disentanglement Services hereunder to the extent applicable to the Terminated Services in such case. Contractor shall be required to perform the Disentanglement Services on an expedited basis, as determined by the County, if the County terminates the Term pursuant to Sections 17.3, 17.4, or 17.5.

6.3. Specific Obligations

The Disentanglement shall include the performance of the following specific obligations (the "Disentanglement Services"):

6.3.1. Disentanglement Plan

Upon Disentanglement, Contractor, the County, and, if applicable, County's designated replacement provider(s) shall discuss in good faith a plan for determining the nature and extent of Contractor's Disentanglement obligations and for the transfer of the Terminated Services in process. Contractor shall within ten (10) days after the commencement of Disentanglement develop, document in detail, and provide the County with a copy of, such Disentanglement plan for County's approval. Upon receipt of County's approval,

Contractor shall promptly implement the Disentanglement plan in accordance with its terms. Contractor's obligation under this Agreement to provide all Services necessary for Disentanglement shall not be lessened in any respect by the Disentanglement plan.

6.3.2. Full Cooperation and Information

The Parties shall cooperate fully with one another and the County's designated replacement provider to facilitate a smooth transition of the Terminated Services being terminated from Contractor to the County or the County's designated replacement provider. Such cooperation shall include the provision (both before and after the cessation of Contractor's providing all or any part of the Terminated Services under this Agreement) by Contractor to the County of full, complete, detailed, and sufficient information (including all information then being utilized by Contractor) to enable the County's personnel (or that of third parties) to fully assume and continue without interruption or adverse impact the provision of the Terminated Services.

6.3.3. No Interruption or Adverse Impact

Contractor shall cooperate with the County and all of the County's other service providers to ensure a smooth transition at the time of Disentanglement, with no interruption of the Terminated Services, no adverse impact on the provision of the Terminated Services or the County's activities, no interruption of any services provided by Third-Parties, and no adverse impact on the provision of services provided by Third-Parties.

6.3.4. Third-Party Authorizations

Without limiting the obligations of Contractor pursuant to Section 15.4, Contractor shall, subject to the terms of any Third-Party contracts, procure at no charge to the County any Third-Party authorizations necessary to grant the County the use and benefit of any Third-Party contracts between Contractor (or its Subcontractors) and Third-Parties used to provide the Terminated Services, pending their assignment to the County pursuant to Section 6.3.7.

6.3.5. Licenses to Software

Contractor acknowledges and agrees that the licenses granted to the County pursuant to Section 15 provide for all Software that would be needed in order to allow the County to continue to perform for itself, or obtain from other providers, the Terminated Services as the same might exist at the time of Disentanglement. Contractor shall also provide the County with a copy of each such program, in such media as requested by the County, together with object code, source code, and appropriate documentation. Contractor shall also offer to the County or its designee the right to receive maintenance (including all updates, upgrades, enhancements, and improvements thereto) and support with respect to such Contractor Works and any and all derivatives thereof for so long as the County requires, at the best rates Contractor is offering to other major customers for services of a similar nature and scope.

6.3.6. Transfer of Assets

Contractor shall convey to the County or its designee, from among those assets then held by Contractor for the provision of the Terminated Services to the County, other than those assets expressly identified by the Parties from time-to-time as Shared Resources such assets as the County may select, at a price consisting of the Net Book Value, calculated in accordance with the guidelines set forth in Schedule 16.14. Contractor shall promptly remove from the County's premises any Contractor assets associated with the Terminated Services that the County, or its designee, chooses not to purchase.

6.3.7. Transfer of Leases, Licenses, and Contracts

Contractor, at its expense, shall convey or assign to the County or its designee such leases, licenses, and other contracts used by Contractor, the County or its designee, or any other Person in connection with the Terminated Services, as the County may select; provided, however, that the Contractor shall convey or assign, and the County or its designee shall accept the conveyance or assignment, of all Desktop Framework Assets at their Net Book Value. Contractor's obligation under this Section 6.3.7 shall include Contractor's performance of all obligations under such leases, licenses, and other contracts to be performed by it with respect to periods prior to the date of conveyance or assignment and Contractor shall reimburse the County for any Losses resulting from any claim that Contractor did not perform any such obligations.

6.3.8. Delivery of Documentation

Promptly upon the commencement of Disentanglement as set forth in Section 6.2, Contractor shall deliver to the County and as applicable, the County's designee, all information and documentation as described in Section 6.4.1.

6.3.9. Hiring of Employees

Contractor shall cooperate with and assist (and shall cause its Subcontractors to cooperate with and assist) the County (or its designee) in offering employment, at the discretion of the County (or its designee), to any or all Contractor employees (and to any or all employees of Contractor's Subcontractors) that are substantially involved in the provision of the Terminated Services whether such offers are made before, at the time of, after, or in anticipation of expiration or termination of the Term. Such cooperation and assistance shall include allowing the County (or its designee) to meet with such employees at Contractor's or its Subcontractor's facilities and providing the County (or its designee) with all relevant and pertinent details regarding the salary and benefits then being received by each Contractor or Subcontractor employee then occupying any such positions or performing any such functions, so as to enable the County (or its designee) to make a reasonable and comparable offer. Contractor shall be solely responsible for, and shall pay, all severance and related payments, if any are payable pursuant to Contractor's standard policies, to any such employees of Contractor hired by the County or its designee, and shall cause the relevant Subcontractor of Contractor to pay severance and related payments, if any are payable pursuant to such Subcontractor's standard policies, to any such employee of a Subcontractor hired by the County (or its designee).

6.3.10. County WARN Notice

If, in the opinion of Contractor, the Disentanglement plan results in a need for a WARN Notice, then Contractor shall so advise the County, and Contractor shall take such action as Contractor deems necessary to provide such WARN Notice. If, pursuant to the Disentanglement Transition Plan, the County informs Contractor in writing that Contractor should not timely provide a WARN Notice to employees, Contractor will refrain from doing so, in which event the County shall be responsible for severance and related costs and expenses arising from the failure to timely provide any required WARN Notice.

6.3.11. Additional Tasks

Upon Disentanglement, Contractor shall perform such additional tasks as may be related to the transfer of the Terminated Services back to the County (or its designee), which shall include, but not be limited to, the performance of the following tasks prior to the Expiration Date:

(a) Contractor shall, within thirty (30) calendar days of County's request, develop and deliver to the County a detailed, accurate and comprehensive list of all Assets used by Contractor or any Subcontractor in connection with the performance of the Terminated Services, which list shall include the location of all such Assets;

(b) Contractor shall, within thirty (30) calendar days of County's request, prepare and pack up any assets located in Contractor or Subcontractor facilities that are associated with the Terminated Services, and that are selected by the County for conveyance to County or its designee; and, Contractor shall remove all such Assets to the dock for shipment to the County (or its designee);

(c) Contractor shall, within thirty (30) calendar days of County's request, prepare, pack up and deliver to the dock for shipment to the County (or its designee), all documentation relating to the Terminated Services;

(d) Contractor shall, within thirty (30) calendar days of County's request, develop and deliver to County (or its designee), a detailed, accurate, current and comprehensive list of all Contractor and Subcontractor personnel supporting the Terminated Services as of and following the commencement of Disentanglement, which list shall include accurate and current contact information for each such person; and

(e) Contractor shall direct such of its personnel and personnel of its Subcontractors, as may be selected by the County, to attend any and all meetings scheduled by the County in connection with Disentanglement and relating to the transfer of the Terminated Services back to the County (or its designee).

6.4. Preparation for Disentanglement

6.4.1. Complete Documentation

Periodically throughout the Term, and at any time upon the County's request, Contractor shall provide to the County (and as part of a Disentanglement, the County's designee(s)) such documentation and other information regarding the performance of Services, or the use, operation, support and maintenance of the Machines and Systems provided via the Services and all Software, Hardware, networks and equipment, as is collectively sufficient

to enable the County, or any reasonably competent Third-Party service provider, to fully assume and continue without interruption or adverse impact the provision of any terminated Services and the use, operation, support, and maintenance use of the Machines, Software and Systems provided via the Services. Contractor shall also provide sufficient documentation for all upgraded or replacement Software, hardware, and network components concurrently with the installation thereof. To the extent that any such documentation relates to Third-Party Works, Contractor shall provide documentation that is of a type generally created in the industry for such Software, hardware, or network components and allows a reasonably competent service provider to reasonably comprehend the proper use, operation, support, and maintenance of such Software, Hardware, or network components. To the extent any such documentation relates to proprietary Contractor Software that is commercially available, Contractor shall provide the County with such documentation as accompanies such commercially available Software, except that if such documentation is insufficient to allow the appropriate personnel of a reasonably competent Third-Party service provider to fully comprehend the use, operation, support, and maintenance of such proprietary Contractor Software, then Contractor shall create and provide the County with sufficient additional documentation in a timely manner, at no charge. Contractor shall destroy all copies of the data and documentation described in this Section that are not turned over to the County; provided, however that Contractor may retain one (1) copy of such documentation and data, excluding the County Data, for archival purposes or warranty support.

6.4.2. Maintenance of Assets

Contractor shall maintain all of the Hardware, Software, Systems, networks, technologies, and other Assets utilized in providing Services to the County (including leased and licensed Assets) in good condition and in such locations and configurations as to be readily identifiable and transferable back to the County or its designees in accordance with the provisions of this Agreement; in addition, Contractor shall insure such Assets in accordance with the requirements of Section 19.

6.4.3. Advance Written Consents

Contractor shall obtain at its own expense, in accordance with Section 15.4 hereof, advance written consents from all licensors and lessors to the conveyance or assignment of licenses and leases to the County (or its designee) in a timely and expedient manner so as to permit Disentanglement in accordance with this Section 6. Contractor shall also obtain for the County the right, upon Disentanglement, to obtain maintenance (including all enhancements and upgrades) and support with respect to the assets that are the subject of such leases and licenses at the price at which, and for so long as, such maintenance and support is made commercially available to other customers of such Third Parties whose consent is being procured hereunder.

6.4.4. All Necessary Cooperation and Actions

Contractor shall provide all cooperation, take such additional actions, and perform such additional tasks, as may be necessary, appropriate or reasonably requested by the County, whether during the Term or during Disentanglement, to ensure a timely and seamless

Disentanglement in compliance with the provisions of this Section 6, including full performance, on or before the Expiration Date, of Contractor's obligations under this Section 6.

PART IV - CONTRACT ADMINISTRATION

7. Administrative Obligations

7.1. Viruses and Disabling Devices

Contractor shall use the better of industry best practices or what it uses for its own business purposes at all times during the Term to identify, screen, and prevent, and shall not itself install, any Disabling Device in resources utilized by Contractor, the County, or any Third-Party, in connection with the Services. A "Disabling Device" is any virus, worm, Trojan horse, timer, clock, counter, time lock, time bomb, or other limiting design, instruction, or routine that could, if triggered, erase data or programming, open to unauthorized use or viewing, or cause the resources to become inoperable or otherwise incapable of being used in the full manner for which such resources were intended to be used. Contractor shall immediately, and at its sole cost and expense, remediate the effects of any Disabling Device discovered in such resources, and shall use any means possible to restore any data altered or destroyed to the condition it was in prior to the impact of the Disabling Device. Contractor shall further take all necessary actions and pay all costs and expenses to remediate damage to the County and third parties, including the County's constituents impacted by the Disabling Device. Nothing in this Section 7.1 shall reduce or alter Contractor's additional indemnity obligations set forth in Section 22.

7.2. End-User Satisfaction and Communication Plan

County may conduct End-User satisfaction surveys during the Term. Contractor shall provide reasonable assistance to County as County may request from time-to-time at no cost to County. Contractor shall also conduct, at no additional cost to County, monthly Service Desk surveys, which are subject to SLs and are more fully described in Schedule 4.8. Additionally, Contractor shall maintain during the Term an End-User communication plan for the County which shall provide, in detail, Contractor's plans for complying with all communication requirements set forth in the Agreement. The communications plan shall be included in the Standards and Procedures Manual. The communication plan shall be reviewed and modified by the Parties, as appropriate, not less frequently than once annually.

7.3. Standards and Procedures Manual

7.3.1. Development of Manual

As specified in the Transition Plan, Contractor shall deliver a reasonable and appropriate draft Standards and Procedures Manual to the County for its review, comment, and approval. At a minimum, the Standards and Procedures Manual should address the topics listed in Schedule 7.3.1. Contractor shall incorporate all comments or suggestions of the County and shall finalize the Standards and Procedures Manual by the dates specified in the Transition Plan. Contractor shall periodically (but not less than monthly) update the Standards and Procedures Manual to reflect changes in the operations or procedures described therein. Updates of the Standards and Procedures Manual shall be provided and

delivered at no cost to the County for review and approval. For purposes of clarity, Contractor shall immediately update the Standards and Procedures Manual when changes are necessary, and shall provide those changes to the County in the periodic update required by this Section 7.3.1.

7.3.2. Content of Manual; Compliance

The Standards and Procedures Manual shall describe how Contractor shall perform the Services under this Agreement, the equipment and software being and to be used, and the documentation (including, e.g., operations manuals, user guides, specifications) that provide further details of such activities. The Standards and Procedures Manual shall describe the activities Contractor shall undertake in order to provide the Services including, where appropriate, direction, supervision, monitoring, staffing, quality assurance, reporting, planning, and oversight activities. The Standards and Procedures Manual is intended to describe to the County how the Services shall be performed and shall in no event be interpreted so as to relieve Contractor of any of its performance obligations under this Agreement. Contractor shall perform the Services in accordance with the County's then current policies and procedures until the Standards and Procedures Manual is finalized and approved by the County in writing. Thereafter, Contractor shall perform the Services in accordance with the Standards and Procedures Manual.

7.4. Contractor Responsibilities for Assets

Contractor shall have sole responsibility for, and shall provide, all care and management, and shall ensure the maintenance, of the Purchased Assets. Contractor shall be fully liable for all loss of or damage to the Purchased Assets, or any other assets used by Contractor or its Subcontractors in the performance of this Agreement. Contractor shall ensure that the assets used in providing the Services shall be properly maintained and protected, normal wear and tear excepted, throughout the Term and shall be insured in accordance with the requirements of Section 19.

7.5. Retained Assets Managed by Contractor

7.5.1. General Obligations Regarding Retained Assets

As of each Cutover Date, Contractor shall be responsible for, and perform all management, administrative, and other obligations set forth in Schedule 4.3 for the Retained Assets under the applicable Service Framework to be performed on or after such Cutover Date. Such obligations shall include responsibility for: (i) the support, maintenance, and management of each Retained Asset (including management performance of the Third-Party contractor with regard to compliance with SLs and other performance metrics); (ii) the compliance with and performance of any operational or contractual obligations imposed on the County or the Contractor with respect to such Retained Assets; (iii) the administration and exercise, as appropriate, of all rights available with respect to such Retained Assets, provided, that Contractor shall not terminate, amend or renew any contract for a Retained Asset without the prior written consent and participation of the County; and (iv) the payment of any fees, penalties, interest or other expenses due and payable with respect to such Retained Assets that are incurred, caused by or result from Contractor's failure to comply with or perform its obligations under this Section 7.5. In performing its obligations set forth in

Schedule 4.3, Contractor will not take any action that would cause the County or Legacy Provider to be in breach of any contract for a Retained Asset.

7.5.2. Particular Obligations for Software Retained Assets

Except with regard to the transfer of Purchased Assets to the County and/or its designee in a Disentanglement, Contractor shall remove or erase all copies of all Software that is a Retained Asset from each Purchased Asset on which such Software is installed prior to: (i) selling or disposing of, in whatever manner, such Purchased Asset; or (ii) using such Purchased Asset for any purpose other than the provision of Services to the County hereunder. Unless otherwise directed by County, Contractor shall in no event transfer any copy of any such Software to any other Machines, nor shall Contractor be able to copy or reproduce such Software. Contractor shall promptly provide the County with a certified and detailed report (including specific identification of Software items removed or erased, and serial numbers of Machines from which so removed or erased) when Contractor removes or erases copies of Software that are Retained Assets in preparation for selling or disposing of, or using for purposes other than the provision of Services to the County, any Purchased Assets on which any such Software is installed. In addition, Contractor shall supply a report to the County during the first month of each quarter setting forth the number of copies of the Software that are Retained Assets that were in use by Contractor during the previous quarter. At least thirty (30) days prior to each date on which any such license fees, or maintenance and support fees, become due and payable by the County to the respective licensors or Third-Party service providers, the County shall provide a written invoice to Contractor setting forth the license fees, or maintenance and support fees, applicable to the copies of the Software that are Retained Assets, that were installed on the Purchased Assets when they were acquired from the County (or Legacy Provider) and, with respect to the applicable time period, the County has not been notified by Contractor that such copies have been removed or erased, which license fees, or maintenance and support fees, shall be determined on a proportionate basis in comparison to the total number of copies for which the County is licensed. Contractor shall pay the County, in cash, the total amount of license fees, or maintenance or support fees, set forth on each such invoice within thirty (30) days after receipt thereof, or, in the County's sole discretion, Contractor shall grant the County a credit in the amount of such license fees toward the Fees set forth on the next invoice submitted by Contractor to the County for the performance of Services hereunder. Further, Contractor shall execute and deliver any and all additional documents and instruments, and take all other actions, that may be necessary to give effect to this Section 7.5.2, including executing and delivering such forms and documents as may be requested, at any time and from time-to-time, with respect to the Retained Assets, whether requested by the County or the respective licensors of the Software that is a Retained Asset.

7.6. Dedicated Resources

All Retained Assets, Purchased Assets, County Software, and any other assets procured by Contractor in connection with the Services, shall be accessed and used only by Contractor and by the Subcontractors identified in Schedule 14.1, and exclusively for the provision of Services to the County and not for Contractor's (or its Subcontractors') internal use or use for the benefit of other customers, unless any such assets will be used by Contractor to provide services to customers in

addition to the County (the "Shared Resources"), as designated on Schedule 7.6, or the County otherwise consents in writing to non-dedicated use.

8. Provision of Resources by the County

8.1. Office Space and Furnishings

The County may make reasonably necessary office space, furnishings, and storage space (the "County Facilities") available to Contractor's on-site personnel performing Services at all Sites throughout the Term and shall maintain the County Facilities in areas and at a level similar to that which it maintained for the employees and subcontractors of the Legacy Provider prior to the applicable Cutover Date; provided that any Contractor personnel shall only perform Services on-site to the extent requested and approved by the County. Contractor is entitled to such space only upon request to County and upon County's written approval which shall take the form and be subject to the terms and conditions of the License Agreement attached hereto as Schedule 8.1. Office space, furnishings, storage space, and Assets installed or operated on County premises and not pursuant to this Agreement, and supplies allocated, are provided "AS IS, WHERE IS," and are to be used exclusively for performance of Services for the County.

8.2. Specific Hardware and Carrier Charges

Contractor shall provide and be responsible for all such telephone and modem lines, telephones, computers and peripheral devices, computer connections, and network access, as may be necessary for Contractor to provide the Services. Contractor shall be responsible for all usage-based carrier charges incurred by Contractor personnel and all usage-based carrier charges incurred to provide a telecommunications link between Contractor and the Locations.

8.3. Access to Personnel and Information

The Parties shall cooperate with each other in all matters relating to Contractor's performance of the Services. With respect to the County, such cooperation shall be limited to providing, as reasonably required by Contractor for the performance of the Services, access to the County's administrative and technical personnel, other similar personnel, and network management records and information.

8.4. Other Facility and Location Related Obligations

(a) Except as expressly provided in this Agreement, Contractor shall use the Locations for the sole and exclusive purpose of providing the Services. Use of Locations by Contractor does not constitute a leasehold interest in favor of Contractor.

(b) Contractor shall use the Locations in a reasonably efficient manner.

(c) Contractor, and its Subcontractors, employees, and agents, shall keep the Locations in good order, shall not commit or permit waste or damage to such facilities, and shall not use such facilities for any unlawful purpose or act. Contractor shall comply with all applicable laws and regulations, including all of the County's standard policies and procedures that are provided to Contractor in writing regarding access to and use of the Locations, including procedures for the physical security of the Locations.

(d) Provided that the County adheres to any mutually agreed upon security procedures implemented by Contractor at the Locations, Contractor shall permit the County and its agents and representatives to enter into those portions of Locations occupied by Contractor staff at any time to perform facilities-related services.

(e) Contractor shall not make any improvements or changes involving structural, mechanical, or electrical alterations to the Locations (including, without limitation, any work affecting any alarm systems at a Location) without the County's prior written approval.

(f) When the County Facilities are no longer required for performance of the Services, Contractor shall return such facilities to the County in substantially the same condition as when Contractor began use of such Facilities, subject to reasonable wear and tear.

(g) Contractor shall not cause the breach of any lease agreements governing use of the Locations.

(h) The County shall provide and maintain, for all County Facilities, adequate heating, ventilation, and air conditioning, electrical connections (to the wall plate), safety and security equipment, and connections to any facility-wide uninterruptible power supply. The County shall provide Contractor with reasonable notice of proposed changes to any of the foregoing that may adversely affect Contractor's Hardware located at any such Facility and, in such cases, Contractor must relocate such Hardware and the County shall reimburse Contractor for its actual costs incurred directly in connection therewith. To the extent provided by the County, the County shall maintain any site-wide uninterruptible power supply that is dedicated to support any County Facility. Contractor shall provide and maintain any uninterruptible power supply dedicated to Contractor's Hardware and shall provide and maintain all connections from the wall plate to the Hardware used to provide the Services.

(i) Contractor shall notify the County's Department of General Services prior to adding or removing any hardware that will require modification of any Locations and shall provide the Department of General Services, for its review and approval, detailed plans and specifications conforming to the Hardware manufacturer's requirements. Contractor shall review and approve all of such Department's changes to the plans and specifications, shall monitor the installation of all approved changes, and shall promptly notify the CIO and the Director of the Department of General Services of any nonconformity with the approved plans and specifications. In addition, whenever the Contractor installs, modifies or removes any wiring or cabling at any County Facility, the Contractor shall annotate the blueprints corresponding to such County Facility and provide the Department of General Services with a set of "as built" blueprints in both electronic and hard copies.

(j) For any Locations added by the County after a Cutover Date, Contractor shall provide the Department of General Services, for its review and approval, detailed plans and specifications conforming to the Hardware manufacturer's requirements that are necessary for Contractor to provide the Services to such Locations.

Contractor shall review and approve all of the Department of General Services' changes, shall cooperate during all phases of the construction or modification of such Locations, and shall promptly notify the CIO and the Director of the Department of General Services of any nonconformity with the approved plans and specifications.

(k) Contractor shall not be responsible for identification or abatement of asbestos-containing material in County-owned or County-controlled Locations. Contractor shall cooperate with the Department of General Services and the County's Department of Environmental Health Services to establish procedures and protocols when performing activities that may disturb or cause the disturbance of asbestos-containing material, including pulling cable, establishing cable runs, or removing floor coverings. Contractor shall provide asbestos-awareness training to all Contractor and Subcontractor employees that perform activities at any Location that could disturb or cause the disturbance of asbestos-containing material.

9. County-Retained Authority

The County shall retain the exclusive right and authority to set the County's IT and telecommunications strategy and to determine, alter, and define any or all of the County's requirements or business processes. The County shall also have the right to approve or reject any and all proposed decisions regarding infrastructure design, technical platform, architecture, and standards and, subject to the change management procedure described in Section 11, will have the right and authority to cause Contractor at any time to change any or all of the foregoing. Contractor shall actively participate in any of the foregoing as the County requests. The County shall consult with Contractor to inform Contractor of significant changes in the County's IT and telecommunications strategy and changes in its requirements and business processes relating to the Services. Contractor shall also provide the County with advice, information, and assistance in identifying and defining IT and telecommunications projects and future IT and telecommunications requirements to meet the County's objectives. Without limiting the generality of the foregoing, the County shall retain exclusive authority, discretion, and rights of approval for the following IT and telecommunications activities:

9.1. Strategic and Operational Planning

Strategic and operational planning, which includes the following:

(a) Developing and implementing policies and architecture pertaining to IT and telecommunication systems for the County, considering alternatives provided by Contractor;

(b) Developing a series of comprehensive standards and planning guidelines pertaining to the development, acquisition, implementation, and oversight and management of IT and telecommunication systems for the County;

(c) Identifying and implementing: (i) optimal IT and telecommunication strategies to efficiently service the needs of the County; and (ii) opportunities for reducing costs for such systems considering alternatives provided by Contractor;

(d) Approving or disapproving, in accordance with guidelines established by the CIO, each proposed County acquisition of Hardware or Software for an IT or telecommunication system;

(e) Approving or disapproving, in accordance with guidelines established by the CIO, all County requests or proposed contracts for consultants for IT and telecommunication systems;

(f) Assessing opportunities for cost savings and greater sharing of IT resources that could result if the District Attorney's Office or the Sheriff's Department acquire IT and telecommunication systems similar to those of the County;

(g) Defining and evaluating IT and telecommunications services including: service availability and minimum acceptable service levels; service specifications, standards, and benchmarking; selection of suppliers; security requirements; scheduling, prioritization, and service conflict resolution among End-Users; Service Desk rules; and general operational management guidelines; and

(h) Service-provider strategy including: selection of providers; specialized provider relationships (e.g., telecommunications); and quality assurance standards.

9.2. Service Design and Delivery

Service design and delivery, which includes the following:

(a) Selecting designs of specific technologies and services from alternatives provided by Contractor;

(b) Selecting specific technologies, Hardware, and Software, from alternatives provided by Contractor, for implementation of such designs;

(c) Selecting providers of specific technologies, Hardware, and Software from alternatives provided by Contractor; and

(d) Selecting implementation schedules and activities from alternatives provided by Contractor.

9.3. Installations, Moves, Adds, and Removes

Ordering Installations, Moves, Adds or Removes with respect to resources used in connection with the Services.

9.4. Applications Development

Designating the County's requirements for applications development and enhancement.

9.5. Business Process Reengineering

Approving Contractor's business process reengineering efforts at the County, coordinating and resolving labor-related issues, and approving performance metrics related to business process reengineering developed by Contractor.

9.6. Contract Management

Managing this Agreement and the County's relationship with Contractor.

9.7. Budget Management

Managing the County's annual budget for all County operations, utilizing Contractor's estimates for services included in the scope of this Agreement and for additional services planned or anticipated throughout the Term.

9.8. Validation and Verification

Performing validation and verification activities in relation to key projects and operational processes.

9.9. Other Retained Authority

Contractor must obtain the prior written authorization of the County before undertaking any activity that is within the exclusive authority of the County pursuant to the terms hereof.

9.10. Review and Acceptance

The CIO, or his designee, on behalf of the County, shall have the right to review and accept or reject all components, deliverables, and systems to be provided by Contractor to the County under this Agreement, pursuant to the methodology set forth in this Section 9.10. Within thirty (30) days after the Effective Date, Contractor shall develop a methodology for the implementation of the process described in this Section 9.10 by the delivery of control documents, the preparation of deliverable acceptance documents, the tracking of accepted deliverables, the maintenance of all deliverables and deliverable acceptance documents, and the development of other documents and processes. The process required by this Section 9.10 shall be set forth in the Standards and Procedures Manual.

9.10.1. Acceptance Process

Upon Contractor's notification to the County that Contractor has completed any component or deliverable identified in this Agreement or in any Service Request or that is developed by Contractor under this Agreement or any Service Request, the County shall begin reviewing the component or deliverable using the review procedures and standards set forth in the Service Request or such other standards as the CIO and Contractor's Account Executive mutually agree in writing ("Acceptance Review Procedures"), to determine whether such component or deliverable meets, in all material respects, the specifications or acceptance criteria set forth in such applicable Service Request or such other criteria as the CIO and Account Executive mutually agree in writing (the "Acceptance Criteria"). After the County has completed such review or upon expiration of the agreed-upon review period specified in the applicable Service Request or such other review period upon which the CIO and Account Executive mutually agree in writing (the "Acceptance Review Period"), the County shall notify Contractor in writing either that: (i) the component or deliverable so meets the Acceptance Criteria and that acceptance of such component or deliverable has occurred ("Acceptance"); or (ii) the Acceptance Criteria have not been met. If the component or deliverable is identified in this Agreement, the applicable Service Request, or in the written specifications developed and mutually agreed upon by the Parties therefor, as being part of a larger, integrated system being developed thereunder, then such Acceptance shall be understood as being conditional acceptance ("Conditional

Acceptance"), and such component or deliverable shall be subject to Final Acceptance in accordance with Section 9.10.3.

9.10.2. Remediation

If the County determines that a component or deliverable does not conform with, in all material respects, the applicable Acceptance Criteria, the County shall promptly deliver to Contractor an exception report describing the nonconformity (the "Exception Report"). Contractor shall promptly investigate the alleged nonconformity and shall correct such nonconformity in all material respects within thirty (30) days of receipt of the Exception Report or, if the nonconformity is incapable of remediation within such thirty (30) day period, Contractor shall present the County, within such 30-day period, a mutually agreeable plan to remediate such nonconformity within a reasonable amount of time. Upon Contractor's notice to the County that Contractor has so remediated such nonconformity, the County shall re-review the defective component or deliverable in accordance with the applicable Acceptance Review Procedures and Acceptance Criteria for an additional review period of up to thirty (30) days or such other period as the CIO and Contractor's Account Executive mutually agree in writing, at the end of which period the process described above in Section 9.10.1 shall be repeated. Contractor shall maintain a "punch list" of Exception Reports submitted by County pursuant to this Section 9.10.2 and shall provide the County with regular reports on its progress on remediating nonconformities identified therein. If the County fails to deliver an Exception Report within thirty (30) days after the expiration of the applicable Acceptance Review Period, the County shall not have the right to withhold any payment that, under this Agreement or a Service Request, is conditioned on Acceptance or Conditional Acceptance, as a result of a claim by the County that the component or deliverable does not conform with the Acceptance Criteria therefor.

9.10.3. Final Acceptance

9.10.3.1. Scope and Intent

Upon completion of (i) all of the Services to be provided under a Service Request, (ii) all components or deliverables that are identified in a Service Request, or (iii) all Services that are performed by Contractor and are subject to Conditional Acceptance, the County shall begin reviewing same, using the review procedures and standards set forth in the applicable Service Request (if any) or such other standards as the CIO and the Contractor's Account Executive mutually agreed upon in writing (the "Final Acceptance Review Procedures"). County's review is intended to determine whether such service, component, deliverable, or system, as applicable, performs as an integrated whole and meets, in all material respects, the specifications or Acceptance Criteria set forth in such applicable Service Request or other standards developed by the Parties and mutually agreed upon in writing by the CIO and Account Executive (the "Final Acceptance Criteria").

9.10.3.2. Acceptance Notification

After the County has completed such review or upon expiration of the review period specified in the applicable Service Request or such other review period as the CIO and Account Executive mutually agree in writing (the "Final Acceptance Review Period"), the County shall notify Contractor in writing that: (1) the system, and all components and deliverables that are a part thereof, meet the Final Acceptance Criteria and that final acceptance of the system and such components and deliverables has occurred ("Final Acceptance"); or (2) that the Final Acceptance Criteria have not been met. If the County determines that the Final Acceptance Criteria have not been so met, the process described in Section 9.10.2 shall be initiated, with all references to "Acceptance Criteria" being references to "Final Acceptance Criteria," all references to "component or deliverable" being references to the "system," all references to "Acceptance Review Procedures" being references to "Final Acceptance Review Procedures," and all references to the "Acceptance Review Period" being references to the "Final Acceptance Review Period." Neither Conditional Acceptance, Acceptance, nor Final Acceptance by the County shall constitute a waiver by the County of any right to assert claims based upon defects not discernable through conduct of the applicable review procedures and subsequently discovered in a component or deliverable or the system within one (1) year of the County's Final Acceptance thereof.

9.10.3.3. No Specified Acceptance Criteria

Upon completion of all of the Services to be provided under a Service Request, to the extent that the Services provided do not result in the development of a system subject to review as stated above, the Final Acceptance Review Procedures shall consist of the County's verification that all of the Services to be provided by Contractor under such Service Request have been provided in all material respects in accordance with the Service Request or such other Acceptance Criteria thereafter developed by the Parties and mutually agreed upon in writing by the CIO and the Account Executive. Contractor shall notify the County when Contractor believes it has so completed the Services under a Service Request. After the County has completed its review of such Services or upon expiration of the agreed-upon review period specified in the applicable Service Request or such other period as the CIO and Account Executive mutually agree in writing, the County shall advise Contractor whether or not the County believes Contractor has so completed such Services. If the County determines that the Services have not been so completed, the County shall promptly deliver to Contractor a written statement describing the reasons therefor. Contractor shall correct such deficiencies in all material respects within thirty (30) days after receipt of such statement or, if the deficiencies are not correctable within such thirty (30) day period, Contractor shall present the County with a mutually agreeable plan to fix such defects within a reasonable amount of time. Upon Contractor's notification to the County that Contractor

has so corrected such deficiencies, the County shall once again determine whether the Services have been so completed within an additional period as agreed in writing by the CIO and the Account Executive, at the end of which the process described in the second and first preceding sentences shall be repeated.

10. RELATIONSHIP MANAGEMENT

10.1. Personnel

10.1.1. A. Contractor Key Personnel

Each of the Contractor Key Personnel shall have the functions assigned to him or her as set forth in Schedule 10.1.1, as such Schedule may be modified from time-to-time in accordance with this Agreement. The County shall have the right to interview, as the County deems necessary, and participate in the selection of, the Contractor Key Personnel and Account Executive, and Contractor shall not (i) designate any Contractor Key Personnel or its Account Executive or (ii) change any Key Personnel without the County's prior written consent. The Parties acknowledge that certain Transitioned Employees will be designated as Contractor Key Personnel by mutual agreement of the Parties before or concurrently with the applicable Cutover Date. Contractor shall obtain the County's prior written consent at least thirty (30) days in advance of any assignment given to any Contractor Key Personnel resulting in the alteration or reduction of time expended by such Contractor Key Personnel in performance of Contractor's duties under this Agreement. If any one of the Contractor Key Personnel is reassigned, becomes incapacitated, the County requests the Contractor Key Personnel's removal pursuant to Section 10.2 or ceases to be employed by Contractor and therefore becomes unable to perform the functions or responsibilities assigned to him or her, Contractor shall, within forty-eight (48) hours, replace such person with another person approved by the County and that is at least as well qualified as the person who initially performed that person's functions. For purposes of this Section 10.1.1, the movement of Contractor Key Personnel from the employ of Contractor to an Affiliate of Contractor shall be considered a reassignment requiring the County's consent and not a cessation of employment.

Upon receipt of a reasonable request from the County, Contractor shall promptly provide resumes to the County for any Contractor Key Personnel performing Services under the Agreement. In addition, upon receipt of a reasonable request from the County, Contractor shall provide the County with resumes for any Contractor personnel providing subject matter expertise in connection with the performance of "complex projects" for the County, which "complex projects" shall be defined as: (i) projects that are estimated to require more than two thousand hours of effort; (ii) projects that introduce new technologies to the County, or (iii) projects that require a high degree of additional integration.

10.1.1 B. Contractor Named Personnel

Each of the Contractor Named Personnel shall have the functions assigned to him or her and documented in Schedule 5 - Report 42, as modified from time-to-time in accordance with this Agreement. The County shall have the right to verify the Named Personnel's

qualifications and skills, and Contractor shall not (i) designate any Contractor Named Personnel or (ii) change any Named Personnel without the County's prior written consent.

10.1.2. Account Executive

Contractor represents and warrants that its Account Executive is an experienced manager who is knowledgeable as to the County's activities and the Services. Notwithstanding anything else herein to the contrary, Contractor shall not replace its Account Executive during the Term without the County's prior written consent. The Account Executive shall act as the primary liaison between Contractor and the CIO, shall have overall responsibility for directing all of Contractor's activities hereunder, and shall be vested by Contractor with all necessary authority to fulfill that responsibility.

10.1.3. CIO

The CIO shall act as the primary liaison between the County and the Contractor's Account Executive and shall have overall responsibility for day-to-day oversight of Contractor's performance under this Agreement and coordination of the County's retained authorities. Notwithstanding the foregoing, the CIO may, in his or her sole discretion, delegate any right or authority hereunder to other employees of the County.

10.1.4. Additional Personnel Requirements

In addition to the Contractor Key Personnel, Contractor shall make available such additional personnel as the County deems necessary to properly perform all of Contractor's obligations under this Agreement.

10.1.5. Minimum Proficiency Levels

Contractor's Key Personnel, and all other personnel assigned by Contractor or its Subcontractors to perform Contractor's obligations under this Agreement, shall have experience, training, and expertise at least equal to the highest commercial standards applicable to such personnel for their responsibilities in the business of providing IT and telecommunications services. Such personnel shall also have sufficient knowledge of the relevant aspects of the Services and of the County's practices and areas of expertise to enable them to properly perform the duties and responsibilities assigned to them in connection with this Agreement. In addition, the Services shall conform to the highest commercial standards applicable to such Services in the IT and telecommunications services marketplace.

10.1.6. Specialized Personnel

Contractor agrees that as part of its provision of Services, it shall ensure that all Contractor personnel (and the personnel of any Subcontractors) are trained, qualified, and available to perform all Services required in work areas requiring specific health, security, or safety precautions.

10.1.7. Training

Contractor shall provide, and cause its Subcontractors to provide, all such training to the employees of Contractor and its Subcontractors (including the Transitioned Employees) as

may be necessary for them to perform, on behalf of Contractor, all of Contractor's duties under this Agreement, and, in any event, levels of training equal to or greater than the average levels of training given to all Contractor employees holding corresponding positions.

10.2. Replacement of Personnel

Notwithstanding Section 10.1.1, if the County believes that the performance or conduct of any Person employed or retained by Contractor to perform Contractor's obligations under this Agreement is unsatisfactory for any reason or is not in compliance with the provisions of this Agreement, the County shall communicate its concerns to Contractor and Contractor shall promptly address the performance or conduct of such person, or, at the County's request, immediately, and at least within the time required by Section 10.1.1, replace such Person with another Person acceptable to the County and with sufficient knowledge and expertise to perform the Services in accordance with this Agreement.

10.3. Relationship Management

Contractor's management structure, roles and responsibilities are set forth in Schedule 10.3.

10.4. Parties' Relationship

From time-to-time during the Term and no less than annually, at the County's request, Contractor shall discuss with the County (and provide reports on) its current financial plans and operational plans related to this Agreement, and Contractor shall make available its senior management personnel to answer questions from the County's senior management personnel regarding such plans.

10.5. Extraordinary Events or Circumstances

The County may, at any time, in a writing signed by the Contracting Officer or his or her designee, and as a result of an extraordinary event or circumstance, including a Force Majeure Event: (i) direct Contractor, in accordance with Section 11, to perform Services in an extraordinary manner (e.g., perform Services at SLs above or below the existing SL requirements for a limited duration); or (ii) direct Contractor to temporarily cease the performance of certain Services; or (iii) obtain a Third-Party to perform certain Services for the duration of the extraordinary event or circumstance. If any such County request causes an increase or decrease in Contractor's direct cost or expense of performance of the affected Services for which Contractor would not otherwise be obligated to provide, the County shall pay Contractor an amount equal to any such increase or Contractor shall credit to the County the amount of any such decrease. Any request by Contractor for such an adjustment must be asserted in writing to the County's Contracting Officer within thirty (30) days after the date of receipt by Contractor of the County's writing with respect to the extraordinary circumstance or event, or within such additional period of time as the County's Contracting Officer may agree in writing, and shall include factual information and support for all purported increases and decreases in direct cost or expense. Pending the determination of any such adjustment, Contractor will diligently proceed with the requested Services. The County may require the submission of supporting cost and expense documentation and inspection of Contractor's pertinent books and records for the purpose of verifying Contractor's request and determining the basis for the adjustment.

10.6. Executive Meetings; Status Meetings

Contractor's Chief Executive Officer shall meet from time-to-time upon the County's written request, with the County's Chief Administrative Officer to review Contractor's performance of the Services and to discuss the status of the relationship between the Parties. During the Term, representatives of the Parties shall meet periodically pursuant to a mutually agreed upon schedule and as otherwise requested by the County to discuss matters arising under this Agreement. Each Party shall bear its own costs in connection with the attendance and participation of such Party's representatives in such meetings. The place and time, and whether to meet via teleconference or in person, shall be as determined by the County.

10.7. Limitation of Future Contracts

The Parties acknowledge and agree that Contractor will be restricted in its future contracting with the County as described in this Section; except as specifically provided herein, Contractor shall be free to compete for future business with the County on an equal basis with other Persons. If Contractor, under the terms of this Agreement, or through the performance of tasks pursuant hereto, develops specifications or statements of work, and such specifications or statements of work are to be incorporated into a County solicitation, Contractor shall be ineligible to perform the work described within that solicitation as a prime contractor or subcontractor under a future County contract.

10.8. Notice of Adverse Impact

Contractor shall immediately inform the County in writing of any failures by Contractor to comply with its obligations under this Agreement, or any other situation, that Contractor is aware of that have resulted, or could reasonably result, in an impact on the (i) Services or the County's operations or the operations of any agency, department or subdivision of the County, (ii) integrity of the County's financial and other internal controls, or (iii) quality, accuracy, integrity, security or confidentiality of County Data. The County may assume that no such circumstances exist unless Contractor so notifies the County.

11. Service Request Procedures; Change Management Procedure

The County shall deliver a Service Request, in the form, and pursuant to and in accordance with the procedures, set forth in the Standards and Procedures Manual; provided that any such procedures contained in the Standards and Procedures Manual shall be consistent with the terms of this Agreement. The Parties understand and agree that all services requested in such Service Requests shall be presumed to be within the scope of the Services and within the Services (and therefore subject to the Maximum Annual Fee). Contractor and its subcontractors and their subcontractors shall perform all Services pursuant to the terms and conditions of this Agreement and shall not be entitled to any additional compensation in addition to or different than provided for under this Agreement, unless expressly allowed in writing by the Contracting Officer. All Service Requests shall be governed by the terms and conditions of this Agreement. A Service Request may alter a SL if and to the extent Contractor's ability to perform at such SL is materially affected by the Service Request, and the County's Contracting Officer has expressly agreed to such alteration in writing. Service Requests must be requested by an authorized representative of the County to be valid. The Parties shall also maintain a mutually agreed-upon change management procedure, which shall be included in the Standards and Procedures Manual.

12. Security and Protection of Information

12.1. Security

12.1.1. Security and Policies

At all times during the Term, Contractor shall provide all Services, and use all resources related thereto, in a secure manner and in accordance with the County's security requirements, including the prevention and detection of fraud, abuse, or other inappropriate use or access of systems and networks by all appropriate means, including network management and maintenance applications and tools, and the use of appropriate encryption technologies. In addition, all Contractor personnel (including personnel of any Subcontractors) shall be subject to and shall at all times conform to the County's laws, rules, and requirements for the protection of premises, materials, equipment, and personnel, as they have been previously disclosed to Contractor in writing, including those set forth on Schedule 12.1.1. Any violations or disregard of these rules shall be cause for denial of access by such personnel to the County's property. Contractor shall exercise due care and diligence to prevent any injury to person or damage to property while on the County's premises. The operation of Contractor vehicles or private vehicles of Contractor personnel on the County's property shall conform to posted and other regulations and safe driving practices. Vehicular accidents on the County's property and involving Contractor personnel shall be reported promptly to the appropriate County security personnel. In addition, the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum ("Security Addendum"), referenced in 28 CFR 20.33 (a)(7), is hereby incorporated by this reference into this Agreement. Contractor acknowledges and agrees that it is bound by all applicable provisions of the Security Addendum. Contractor and the County further agree that, in accordance with Section 5.05 of the Security Addendum, the County does not anticipate and will not authorize any requests to Contractor for the criminal history record information covered by the Security Addendum, because Contractor is performing an IT support function.

The following California Law Enforcement Telecommunications System ("CLETS") documents are hereby incorporated by reference into this Agreement.

(a) California Law Enforcement Telecommunications Systems (CLETS) Policies Practices, Procedures and Statutes, Rev 11/99, and further revisions as necessary.

(b) CLETS Computer Interface Rules and Requirements, Rev 09/95, and further revisions as necessary.

Contractor will also comply with the applicable provisions of the CLETS documents and the FBI Criminal Justice Information Services Security Addendum included in Exhibit 12.1.1-1, CLETS System Security Requirements.

Contractor shall ensure that all persons having access to the CLETS system as defined by the CLETS documents shall have first obtained the required background investigation and clearance, as conducted and approved by the Sheriff. Contractor acknowledges and agrees that the operation, policy, planning, and training for the CLETS system shall be subject to the oversight and authority of the Sheriff. In cases of alleged violation of CLETS policy

and procedures, appropriate corrective actions, if any, will be coordinated with the Sheriff and the County Technology Office to ensure appropriate disciplinary action is taken, as mutually agreed.

Any amendments to the terms and conditions of the Agreement relating to the CLETS system shall be coordinated with the Sheriff and the County Technology Office, and shall not be effective without the approval and signature of the Sheriff.

12.1.2. Information Access

Prior to performing any Services, Contractor personnel who will access County computer data and software, including the County Data, shall execute the Parties' agreements and forms concerning access protection and data/software security consistent with the terms and conditions of this Agreement. Contractor promises that at all times during the Term, it, and its employees, agents, and Subcontractors, shall comply with all County policies and procedures regarding data access and security, including those prohibiting or restricting remote access to County systems and data. The County shall authorize and Contractor shall issue any necessary information-access mechanisms, including access IDs and passwords, and Contractor promises that the same shall be used only by the personnel to whom they are issued. Contractor shall provide to such personnel only such level of access as is required to perform the tasks and functions for which such personnel are responsible. Contractor shall from time-to-time, upon request from the County but at least quarterly, provide the County at no additional charge with an updated list of those Contractor and Subcontractor personnel having access to the County's systems, software, and data. Computer data and software, including the County Data, provided by the County or accessed by Contractor or Subcontractor personnel, shall be used by Contractor or Subcontractor personnel only in connection with Contractor's obligations hereunder, and shall not be commercially exploited by Contractor or any Subcontractor in any manner whatsoever. In addition, failure of Contractor or any Subcontractor to comply with the provisions of this Section 12 may result in the County restricting offending personnel from access to County computer systems or County Data, or immediate termination of this Agreement pursuant to Section 17.3. Contractor and each Subcontractor shall at all times maintain and ensure the confidentiality and security of the County Data.

12.1.3. Background Checks

If Contractor assigns Persons (whether employees, independent contractors, or agents) to perform Services at any Location, Contractor shall conduct a background check, as permitted by law, on all such Persons before the County will grant access to such Location or such Person will be escorted by Contractor personnel who have passed the background check conducted by the Contractor. Such background check shall be in the form generally used by Contractor in its initial hiring of employees or contracting for independent contractors, as applicable, during the employment-screening process but must, at a minimum, have been performed within the preceding twelve (12) month period and detail the individual's arrest record and employment history. Contractor shall obtain all releases, waivers, or permissions required for the release of such information to the County. On an annual basis, Contractor's human resources manager for this Agreement shall certify that

the background check required by this Section 12.1.3 and any other background check requirement set forth in the Agreement has been conducted in respect of all Persons assigned by Contractor to perform work at any Location. In addition to the background check requirement set forth in this Section 12.1.3, Contractor shall also perform any other background checks required by any other provision of this Agreement, including, but not limited to the background checks required by Schedule 12.1.1.

12.1.4. Other Policies

Contractor shall, and shall cause its Subcontractors and employees to, abide by all County policies that may be established by the County from time-to-time, and which are either provided to Contractor in writing or made available to the Contractor via the County's website. The County shall have no obligation to notify the Contractor of changes and updates to County policies and Contractor shall be responsible to review the County's website for such updates or changes posted by the County from time-to-time.

12.1.5. Minimum Security Standards and Audit

In no event shall Contractor's actions or inaction result in any situation that is less secure than either: (i) the security the County and the Legacy Provider provided with respect to the applicable Service Framework as of the Cutover Date for such Service Framework; the security required by this Agreement; or (iii) the security Contractor then provides for its own systems and data. At any time and from time-to-time, upon reasonable notice, the County may engage any organization as it may deem suitable to conduct an audit of the IT and telecommunications environment used to provide the Services, including security, policies, and operational matters. Any such audit shall be scheduled so as to minimize the disruption to Contractor's business operation.

12.2. Protection of County Confidential Information

12.2.1. Nondisclosure; Contractor Policies and Procedures

(a) All County Confidential Information shall be deemed the sole property of the County furnishing the same, shall be deemed confidential and proprietary to the County, shall be used solely by Contractor or any of its Subcontractors for the purpose of performing its obligations under this Agreement, and shall not be published, transmitted, released, or disclosed by Contractor or its Subcontractors to any other Person without the prior written consent of the County, which consent the County may withhold in its sole discretion.

(b) Contractor shall implement and maintain appropriate policies and procedures to safeguard the confidentiality of the County Confidential Information in accordance with this Section 12 and Schedule 12.1.1, including the policies, procedures and requirements described in Sections 12.1.1, 12.1.2, 12.1.3 and 12.1.4 hereof. Further, Contractor shall comply, and require its employees to comply, with the provisions of Section 10850 of the California Welfare and Institutions Code. Contractor shall require as a condition of any subcontract that the Subcontractor expressly acknowledges and agrees to be bound by the same confidentiality requirements (including any applicable laws pertaining to confidentiality) by which Contractor is bound under this Agreement.

12.2.2. Disclosure Requests

Any and all requests, from whatever source, for copies of or access to, or other disclosure of, any County Confidential Information shall be promptly submitted to the County for disposition.

12.2.3. Permitted Disclosure

Notwithstanding the above provisions of this Section 12.2, Contractor may disclose County Confidential Information to its employees, agents, and Subcontractors who have: (i) a need to know such County Confidential Information in order to perform their duties under this Agreement, as determined by an appropriate County official; (ii) a legal duty to protect the County Confidential Information; and (iii) have complied with any background check and security requirements required by this Agreement. Contractor shall be fully liable for the acts or omissions of its Subcontractors and employees with respect to such County Confidential Information.

12.2.4. Publicity

Contractor shall not release any information concerning this Agreement, the Services or any part thereof to any member of the public or the press or any representative of any business entity or official body, unless prior written consent is obtained from the County.

12.3. Protection of Public Record Data

12.3.1. No Ownership by Contractor

Neither Contractor, nor its Subcontractors, employees, or agents, shall have any ownership rights or interest in any Public Record Data that they possess, modify, or create pursuant to this Agreement, or any modifications thereto or derivatives thereof, all of which shall, at all times and for all purposes, remain the property of the County.

12.3.2. No Impairment by Contractor

Neither Contractor, nor its Subcontractors, employees, or agents, shall impair the integrity of any Public Record Data that they possess or create.

12.3.3. California Public Records Act

Any Public Record Data that is provided to Contractor, or its Subcontractors, employees, or agents, shall remain a public record for purposes of the California Public Records Act (Governmental Code §6250, et. seq.) (the "California Public Records Act"). Contractor, and its Subcontractors, employees, and agents, shall have a joint and several obligation to comply with the obligations of the County under the California Public Records Act as amended, with regard to the Public Record Data and the management, handling, retention, destruction, transfer, and disposal thereof. The determination of whether to disclose any such data shall be made solely by the County.

12.3.4. Limitations on Disclosure

Neither Contractor nor its Subcontractors, employees, or agents, shall disclose to the public any Public Record Data that they possess, modify, or create pursuant to this Agreement and

which the County: (i) is prohibited in disclosing pursuant to federal, State, or County law or regulation; (ii) may disclose pursuant to federal, State, or County law or regulation only to certain Persons or under certain conditions; or (iii) may withhold from disclosure pursuant to federal, State, or County law or regulation. No provisions of this subsection shall be construed to prohibit Contractor from disclosing such Public Record Data to any Subcontractor if necessary to carry out the purposes of this Agreement; provided, however, that Contractor's Subcontractors shall comply with any background check and security requirements required by this Agreement prior to such disclosure(s). In no event shall Contractor, or its Subcontractors, employees, or agents, sell, market, or otherwise profit in any manner from the disclosure or use of any Public Record Data.

12.3.5. Notification

If Contractor learns of any violations of this Section 12.3, it shall promptly (and in no event later than seven (7) days, or sooner if otherwise required by this Agreement, after learning of such violation) notify the CIO of such violation. In addition to any Indemnification required by Section 22, and without waiving any other remedy available to the County in law and equity, Contractor shall provide or cause to be provided, at its sole expense, commercially available identity theft protection to any Person impacted where there has been a violation of this Section 12.3.

12.4. Legally Required Disclosure

Either Party may disclose Confidential Information of the other Party to the extent disclosure is based on the good faith written opinion of such Party's legal counsel that disclosure is required by law or by order of a court or governmental agency; provided, however, that such Party shall give prompt notice of such requirement and use its best efforts to assist the owner of such Confidential Information if the owner wishes to obtain a protective order or otherwise protect the confidentiality of such Confidential Information. The owner of such Confidential Information reserves the right to obtain a protective order or otherwise protect the confidentiality of such Confidential Information. For purposes of this Section 12.4, the County's Office of the County Counsel shall act as the County's legal counsel.

12.5. Notification

In the event of any disclosure, loss, or destruction of Confidential Information, the receiving Party shall immediately notify the disclosing Party. This notification requirement is in addition to any other notification requirement(s) set forth in the Agreement.

12.6. Injunctive Relief

If Contractor publishes, transmits, releases, or discloses any County Confidential Information in violation of this Section 12, or if the County anticipates that Contractor shall violate or continue to violate any restriction set forth in this Section 12, the County shall have the right to have the provisions of this Section 12 specifically enforced by any court having equity jurisdiction, without being required to post bond or other security and without having to prove the inadequacy of available remedies at law, it being acknowledged and agreed that any such violation shall cause irreparable injury to the County and that monetary damages shall not provide an adequate remedy to it. In addition, the County and any individuals that were the subject of such County Confidential

Information may take all such other actions and shall have such other remedies available to it or them at law or in equity and shall be entitled to such damages as it or they can show have been sustained by reason of such violation.

12.7. Return of County Confidential Information

Promptly upon the expiration or termination of the Term, and at any other time upon written request by the County to Contractor, Contractor shall promptly return to the sole custody of the County or to County's designee, all County Confidential Information then in its possession or control, in whatever form, or, in the case of written request by the County, such County Confidential Information specified in such request as then in its possession or control, in whatever form. In addition, unless the County otherwise consents in writing, the Contractor shall also deliver to the County or to County's designee or, if requested by the County, shall delete or destroy, any copies, duplicates, summaries, abstracts, or other representations of any such County Confidential Information or any part thereof, in whatever form, then in the possession or control of the other Party. Contractor shall at all times comply in all respects with the California Public Records Act with regard to its return or destruction of any Public Record Data.

12.8. Confidentiality Agreements and Training

Contractor shall require each of its employees, agents, and Subcontractors providing Services hereunder or otherwise having access, in whatever form or function, to the data and information collected, received, stored, or transmitted pursuant to this Agreement, including the County Data, to execute, prior to any activity or access, an agreement in form and substance acceptable to the County under which such employees, agents, and Subcontractors agree to protect all County Confidential Information. Contractor shall also require employees, agents, and Subcontractors providing Services hereunder or otherwise having access, in whatever form or function, to the data and information collected, received, stored, or transmitted pursuant to this Agreement, including the County Data, to successfully complete any County-required training. The confidentiality agreements and training required by this Section 12.8 shall be in addition to and not in place of any other confidentiality or similar agreements or training required by this Agreement.

12.9. Statutory Requirements Prevail

In the event of a conflict between the provisions of the California Public Records Act, or any other law, and this Agreement, the provisions of such law shall prevail.

12.10. Contractor Confidential Information

The County shall use the same care to prevent disclosure of the records, data, and other information that is obtained by the County in confidence from Contractor or its Subcontractors in connection with its performance of this Agreement, whether oral, written, recorded on electronic media, or otherwise, and including all financial information, personnel information, reports, documents, correspondence, plans, and specifications, and other records, data, or information collected, received, stored, or transmitted in any manner, and that are exempt from disclosure under the California Public Records Act (collectively, the "Contractor Confidential Information"), as it uses to prevent disclosure of its own information of a similar nature, but in no event less than a reasonable degree of care. Contractor Confidential Information shall not include information that the County can demonstrate was: (i) at the time of disclosure to the County, in the public domain;

(ii) after disclosure to the County, published or otherwise made a part of the public domain through no fault of the County; (iii) in the possession of the County at the time of disclosure to it, if the County was not then under an obligation of confidentiality with respect thereto; (iv) received after disclosure by Contractor to the County from a Third-Party who had a lawful right to disclose such information to the County; or (v) independently developed by the County without reference to Contractor Confidential Information. For purposes of this provision, information is in the public domain if it is generally known (through no fault of the County) to third parties who are not subject to nondisclosure restrictions similar to those in this Agreement.

13. Recordkeeping and Audit Rights

13.1. Recordkeeping

Contractor shall maintain complete and accurate records and books of account with respect to this Agreement utilizing generally accepted accounting principles ("GAAP"), consistently applied and complying in all respects with all applicable County, State, or federal laws or regulations. Such records and books, and the accounting controls related thereto shall be sufficient to provide reasonable assurance that:

(a) transactions are recorded so as to permit the preparation of Contractor's financial statements in accordance with GAAP and to maintain accountability for its assets; and

(b) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

Such records and books of account of Contractor's business shall be maintained by Contractor at its primary business office in San Diego, California and the County may examine and make extracts of information and copy any part thereof at any reasonable time during normal business hours. Contractor shall retain and maintain accurate records and documents relating to performance of Services under this Agreement until the latest of: (i) six (6) years after the final payment by the County to Contractor hereunder; (ii) one (1) year following the final resolution of all audits or the conclusion of any litigation with respect to this Agreement; or (iii) such longer time period as may be required by applicable law or regulation.

13.2. Operational Audit Rights

The County, or its authorized representatives shall have the right, at any time and with reasonable notice, to perform an operational or security audit with respect to Contractor's performance hereunder. Contractor shall grant County, or its authorized representative the right to conduct audits of Contractor's and its Subcontractors' practices, the facilities used by Contractor or its Subcontractors to provide the Services, and related operational matters (including audits of Contractor's legal compliance and Contractor's security policies and practices with regard to IT and data access and control) in order to verify compliance with the terms of this Agreement. Any such audit shall be conducted in a reasonable manner and after reasonable advance notice (except that no notice shall be required with respect to a security audit).

For purposes of such audit, Contractor shall, and shall cause its Subcontractors to provide the County and its representatives such information and assistance as requested in order to perform such audits, including full and complete access to personnel, and all books, records, documents,

data, or information as may be required in order for the County to ascertain any facts relevant to Contractor's and its Subcontractor's operational and security obligations hereunder. Contractor shall provide to County any security audits, including, but not limited to SAS 70, and which relate directly or indirectly to any of the Services. If any such audit reveals an inadequacy or deficiency in Contractor's performance, including performance in connection with any security obligations of Contractor as set forth in this Agreement, Contractor shall promptly develop and provide to the County a reasonable and detailed corrective action plan, for the County's approval, and promptly thereafter implement such plan in accordance with its terms. In addition, the cost of such audit, should inadequacies or deficiencies be revealed, shall be borne by Contractor. In all circumstances, the Contractor and its Subcontractors shall be responsible for each of their costs and expenses incurred in connection with any audit performed under this Agreement. At the County's request, Contractor shall provide the County with copies of all documents, data, or information in the possession or control of Contractor that pertain to the Services. Contractor shall provide such documents, data, or information on such media as the County might request, including hard copy, optical or magnetic disk, or tape. Contractor shall incorporate this paragraph verbatim into any Agreement into which it enters with any Subcontractor providing Services under this Agreement.

14. Use of Affiliates and Subcontractors

14.1. Approval; Key Subcontractors

Contractor shall not perform the Services through its Affiliates or through the use of Contractor-selected subcontractors, including providers of Hardware and Software, without the advance written consent of the CIO as to the selection of the subcontractor, which consent may be withheld in the CIO's sole discretion; provided, however, that Contractor may subcontract, without the CIO's advance written consent, for goods and services that are incidental to the performance of the Services and do not involve the anticipated expenditure under this Agreement of more than two hundred fifty thousand dollars ($250,000.00) within any ninety (90) day period. The CIO hereby consents to the Subcontractors identified in Schedule 14.1. Additionally, each Subcontractor shall be properly licensed in the State to perform the Services for which such Subcontractor is responsible. Contractor agrees that it shall continue throughout the Term to retain the Subcontractors identified as "Key Subcontractors" in Schedule 14.1, and that such Persons shall continue to provide the Services initially provided, unless Contractor has obtained the County's prior written consent, which may be withheld in the County's sole discretion. In the event that the Contractor desires to subcontract a particular Service in accordance with this Section, the County may require that such a Service be provided by a certain Subcontractor. In no event shall Contractor be entitled to perform the Services through the use of any subcontractor who has been suspended or disbarred (or who employs a Person or Persons that have been suspended or disbarred) from performing services for the United States government. The CIO, in his or her sole discretion, is authorized to remove or add subcontractors as Key Subcontractors to Schedule 14.1 during the Term.

14.2. Subcontractor Agreements

Contractor shall provide, upon request, to the County copies of all agreements between Contractor and its Subcontractors related to the performance of this Agreement that are in excess of two hundred fifty thousand dollars ($250,000.00) within thirty (30) days after such contracts are

executed by Contractor and its Subcontractors. Contractor represents and warrants that the agreements provided to the County will be true and complete copies thereof, excluding only relevant pricing information between Contractor and its Subcontractors. All subcontracts will contain materially the same terms and conditions as this Agreement.

14.3. Liability and Replacement

In no event shall Contractor be relieved of its obligations under this Agreement as a result of its use of any Subcontractors. Contractor shall supervise the activities and performance of each Subcontractor. If the County determines that the performance or conduct of any Subcontractor is unsatisfactory, the County may notify Contractor of its determination in writing, indicating the reasons therefor, in which event Contractor shall promptly take all necessary actions to remedy the performance or conduct of such Subcontractor or to promptly replace such Subcontractor by another Third-Party or by Contractor personnel.

14.4. Subcontractor Liability

Without limiting Contractor's obligations as the prime contractor hereunder, Contractor acknowledges and agrees that, subject to the Limitation of Liability set forth in Section 18.2, Contractor shall be responsible for the actions of its subcontractors.

14.5. Direct Agreements

At any time and for any reason, including, but not limited to, the expiration or termination of the Term of the Agreement or any part thereof or under any other circumstance in which the County may desire, in its sole discretion, to direct Contractor to use a Subcontractor to perform any Services or to directly engage any Subcontractor to perform any Services then being performed by Contractor or which County seeks to have performed, the County shall have the right to negotiate with, and enter into direct agreements with, any Subcontractor(s). Contractor represents, warrants, and agrees that its arrangements with such Subcontractors will not prohibit or restrict such Subcontractors from negotiating with the County or entering into direct agreements with the County.

15. Proprietary Rights

15.1. County Works

15.1.1. Ownership by the County

All County Works, including all Intellectual Property Rights in or pertaining to the same, shall be owned solely and exclusively by the County or its Third-Party licensors, as applicable. Nothing in this Agreement transfers any ownership or title in or to any County Works to Contractor or any other Person.

15.1.2. License Grant to Contractor

As of the Cutover Date for each Service Framework, the County hereby grants to the Contractor a limited, non-exclusive, non-transferable, royalty-free right and license to use solely those County Works provided to Contractor pertaining to such applicable Service Framework during the Term and any period of Disentanglement, to the extent necessary and appropriate for the sole purpose of Contractor performing the Services, subject to, and

as provided for by, the terms and conditions of this Agreement. Contractor acknowledges that the County Works represent the valuable, intellectual property of the County (or its licensors). To the extent necessary for Contractor to provide the Services, such license grant extends to Subcontractors designated by Contractor that sign a written agreement to be bound by all of the terms contained herein applicable to the County Works. To the extent any County Works are comprised of Third-Party Works, such license grant shall be subject to Contractor having obtained any Required Consents. Contractor and its Subcontractors shall not (i) use any of the County Works for the benefit of any Person other than the County, (ii) reverse assemble, reverse engineer, translate, disassemble, decompile any of the County Works without the prior written approval of the County, which may be withheld in the County's sole discretion, or (iii) in violation of any license for Third-Party Works.

15.2. Contractor Works

15.2.1. Ownership by Contractor

All Contractor Works, including all Intellectual Property Rights in or pertaining to the same, shall be owned solely and exclusively by Contractor. Nothing in this Agreement transfers any ownership or title in or to any Contractor Works to County or any other Person.

15.2.2. License Grant to the County

Contractor hereby grants to the County (and any Third-Party providers of services to the County) a perpetual, irrevocable, non-exclusive, worldwide, fully paid, royalty-free license, including any moral rights, to access, use, modify, copy, adapt, display, perform and create derivative works of, the Contractor Works provided or made available to the County or otherwise used by Contractor or its Subcontractors in connection with the Services (including, but not limited to, all updates, upgrades, enhancements and improvements thereto), as necessary and appropriate for the conduct of the County's business, administration and operations or for the County to receive the full benefit of the Services during the Term and any period of Disentanglement, and thereafter solely for the conduct of the County's business, administration and operations, and not for commercial exploitation or resale. Contractor's obligations with respect to the provision of updates, upgrades, enhancements and improvements upon Disentanglement shall be as set forth in Section 6.3.5.

15.3. Work Product

15.3.1. County Sole Owner

All Work Product, including all Intellectual Property Rights in or pertaining to the same, shall be owned solely and exclusively by the County. Nothing in this Agreement transfers any ownership or title in or to any Work Product to Contractor or any other Person. Ownership of Work Product shall inure to the benefit of the County from the date of conception, creation, or fixation in a tangible medium of expression (whichever occurs first), of such Work Product. Contractor (1) agrees that all copyrightable aspects of such Work Product shall be considered "work made for hire" within the meaning of the Copyright Act of 1976, as amended, (2) hereby assigns to the County exclusively all right,

title, and interest in and to such Work Product, and all copies thereof, and the Intellectual Property Rights therein, that it may have or obtain, without further consideration, free from any claim, lien for balance due, or rights of retention thereto on the part of Contractor or any other Person, and (3) acknowledges that the Parties do not intend Contractor to be a joint author of such Work Product within the meaning of the Copyright Act of 1976, as amended, and that in no event shall Contractor be deemed a joint author of such Work Product. Contractor shall obtain similar written undertakings from all Subcontractors, employees and consultants who will perform any Services, so as to ensure the County's ownership of the Work Product as provided herein, and shall not commence the deployment of any such Subcontractor, employee or consultant until Contractor has obtained such a written undertaking.

15.3.2. Embedded Contractor Works

To the extent that any Contractor Works are incorporated into, embedded or used in or made part of the Work Product, notwithstanding Section 15.3.1 to the contrary, Contractor hereby grants to the County (and any Third-Party providers of services to the County) a perpetual, irrevocable, non-exclusive, worldwide, fully paid, royalty-free license, including moral rights, to access, use, modify, copy, adapt, display, perform and create derivative works of, such Contractor Works and to make, have made, use and sell any inventions therein, all to the extent necessary to give the County unrestricted use and enjoyment of such Work Product and all Intellectual Property Rights therein.

15.3.3. License Grant to Contractor

The County hereby grants to Contractor a limited, non-exclusive, non-transferable, royalty-free right and license to use the Work Product during the Term and any period of Disentanglement, to the extent necessary and appropriate for the sole purpose of Contractor's performing the Services, subject to, and as provided for by, the terms and conditions of this Agreement. To the extent necessary for Contractor to provide the Services, such license grant extends to Subcontractors designated by Contractor that sign a written agreement to be bound by all of the terms contained herein applicable to the Work Product. Contractor and its Subcontractors shall not (i) use any of the Work Product for the benefit of any Person other than the County, or (ii) reverse assemble, reverse engineer, translate, disassemble, decompile any of the Work Product without the prior approval of the County, which may be withheld in the County's sole discretion.

15.3.4. Intellectual Property Protection

Contractor shall promptly and fully disclose and deliver all Work Product to the County, in writing and (with respect to computer programs) in both source code and object code form and with all available user manuals and other documentation, as requested by the County, and shall execute and deliver any and all patent, copyright, or other applications, assignments, and other documents that the County requests for protecting the Work Product, whether in the United States or any other country. The County shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Contractor shall cooperate, as part of the Services, in the preparation and prosecution of all such applications and in any legal actions and proceedings

concerning the Work Product. Contractor shall provide to the County, on a quarterly basis, and at no additional charge, a written report summarizing all of the Work Product developed by Contractor to date, with appropriate information to enable the County to pursue all intellectual property registrations or other protections for the County's interests in the Work Product. The County shall have unrestricted access to all Contractor materials, premises and computer files containing the Work Product.

15.4. Third-Party Works

Unless otherwise provided in this Agreement or expressly and mutually agreed to by the Parties in writing, Contractor shall not implement or utilize any Third-Party Works in the provision of any Services unless Contractor shall have secured for the County (and any Third-Party providers of services to the County) a perpetual, irrevocable, non-exclusive, royalty-free, fully paid-up, worldwide license, including moral rights, to access, use, modify, copy, adapt, display, perform and create derivative works of, and otherwise receive the benefit of, such Third-Party Works as necessary and appropriate for the conduct of the County's business, administration and operations or for the County to receive the full benefit of the Services. Further, Contractor shall not embed any Third-Party Works in any Work Product, or create a derivative work of any Third-Party Work as Work Product, without the express, prior written consent of the County. Contractor's obligations with respect to the provision of updates, upgrades, enhancements and improvements upon Disentanglement shall be as set forth in Section 6.3.5

15.5. Residuals

Notwithstanding anything to the contrary provided in this Agreement, Contractor shall not be precluded from using its Residuals, provided that Contractor's right hereunder to use any of its Residuals that are components of Work Product shall not affect, alter, limit, or interfere with any provisions of this Section 15 that provide for ownership of the Work Product itself, or the Intellectual Property Rights in or pertaining thereto, by the County.

15.6. No Limitation of Governmental Rights

Certain federal or State of California agencies or other governmental entities that provide funds to the County or in connection with the County's activities and undertakings may have certain rights in the Work Product that arise under federal or State law. Therefore, Contractor hereby grants each such governmental agency or entity such rights in and to the Work Product as such agency or entity is entitled to by applicable law. Each Party expressly acknowledges and agrees that all rights granted, retained, or otherwise allocated pursuant to this Section 15.6 are expressly subject and subordinate to such rights as may be reserved or granted to such federal or State agencies or other governmental entities by law and that nothing in this Agreement shall or shall be construed to in any way limit such governmental rights, which rights shall take precedence over this Agreement in the event of any conflict.

15.7. Rights and Licenses

15.7.1. Necessary to the Services

Contractor shall obtain from third parties all rights and licenses required to perform the Services, and the terms and conditions of all such rights and licenses shall be subject to the

review and approval of the CIO prior to their implementation by Contractor. With respect to all technology used and to be used by Contractor to perform the Services hereunder, whether proprietary to Contractor or to any other Person, Contractor hereby grants and agrees to grant to the County, or shall cause to be granted by the licensor thereof, as the case may be, without additional charge, such licenses and sublicenses as may be necessary in order for the County, and its authorized representatives (including Third-Party service providers), to use, or receive the benefit of the use by Contractor of, such technology in connection with the Services.

15.7.2. Advance Consents

Contractor shall obtain advance consents from Contractor's licensors and lessors to the conveyance or assignment, at no cost to the County, of all licenses and leases related to the Services to the County upon Disentanglement. If such advance consents cannot be obtained during Disentanglement, Contractor shall (i) promptly notify the CIO of which Third-Party authorizations or consents it is unable to obtain; (ii) use all commercially reasonable efforts to identify reasonable, alternative sources of goods, services, or Software comparable to those being provided under each such licenses or leases, at a comparable or lower price; and (iii) consult with the County regarding such identified alternatives and, to the extent the County approves of such alternatives in writing, proceed to procure and implement such alternatives on behalf of the County, at no cost to the County, provided that the County shall have the option to enter into the applicable license or lease in its own name.

15.8. County Data

The County shall permit Contractor to have access to the County Data solely to the extent Contractor requires such access to such data to provide the Services and maintain the SLs. Contractor may only access and process the County Data in connection herewith or as directed by the County in writing and may not otherwise modify the County Data, merge it with other data, commercially exploit it, or do any other thing that may in any manner adversely affect the integrity, security, or confidentiality of such data, other than as specified herein or as directed by the County in writing. Contractor understands and agrees that the County owns all right, title, and interest in the County Data, and also owns all copyright, trademark, trade secrets, and other proprietary rights in the County Data. Contractor agrees that all copyrightable aspects of such County Data shall be considered "work made for hire" within the meaning of the Copyright Act of 1976, as amended. Contractor hereby assigns to the County exclusively all right, title, and interest in and to the County Data and to all Intellectual Property Rights therein, without further consideration, free from any claim, lien for balance due, or rights of retention thereto on the part of Contractor. Contractor also acknowledges that the Parties do not intend Contractor to be a joint author of the County Data within the meaning of the Copyright Act of 1976, as amended, and that in no event shall Contractor be deemed a joint author thereof. Furthermore, Contractor and all Subcontractors will not publish or disclose in any manner privacy and security safeguards related to any federal, State, or County data or any other data of which Contractor or any Subcontractor has custody. In no event shall Contractor withhold County Data from, or deny access thereto by, the County in connection with any dispute between the Parties.

15.9. Cooperation

If at any time either Party brings, or investigates the possibility of bringing, any claim against any third-party for infringement of any Intellectual Property Right of such Party, including misappropriation of trade secrets and improper use or disclosure of Confidential Information, then the other Party, upon the request and at the expense of the requesting Party, shall cooperate with and assist such requesting Party in the investigation or pursuit of such claim and provide such requesting Party with any information in its possession that may be of use to such requesting Party in the investigation or pursuit of such claim. Notwithstanding the foregoing, if an Affiliate, client, customer, or other business associate of a Party becomes the subject of such an investigation by the requesting Party, such Party will provide reasonable cooperation to the requesting Party, to the extent not inconsistent with such Party's legal and contractual obligations to such Affiliate, client, customer, or business associate.

PART V – PRICING

16. Financial Terms

As the sole and entire financial consideration for all of the Services to be performed by Contractor and for all of the other tasks, services, and obligations of Contractor under this Agreement, the County shall pay to Contractor the amounts set forth in this Section 16. Except as specifically provided in Section 16.1.4, below, at no time and under no circumstance shall the County pay Fees in any Contract Year that exceed, in the aggregate, the Maximum Annual Fee, as determined in accordance with such Section, for such Contract Year. No work performed by Contractor for the County between the Signing Date and the date on which Contractor formally commences performance of Transition Services in order for Contractor to be prepared for a smooth cutover of operational responsibility for the Services, including work in preparation for accomplishment of the Transition, shall obligate the County to make any payments to Contractor.

16.1. Fees

16.1.1. Transition Milestone Payments

The County shall pay the Fees associated with the Transition of a particular Service Framework as set forth in Section 4 of Schedule 16.1.

16.1.2. Monthly Services Charge

The County shall pay the Monthly Services Charge in arrears in accordance with the terms and conditions of this Agreement and as set forth in Schedule 16.1.

16.1.3. RESERVED

16.1.4. Maximum Annual Fee

(a) Within thirty (30) days prior to the end of each Contract Year, the County shall determine, in its sole discretion, the Maximum Annual Fee for the forthcoming Contract Year, and shall notify Contractor of such amount. Such amount shall be based, in part, upon the County and Contractor's projection of the County's requirements for Services for such Contract Year and shall be subject to annual appropriations by the County of sufficient funds. Each Contract Year, the

Maximum Annual Fee shall be memorialized in writing in a revised Exhibit 16.1-3 to Schedule 16.1.

(b) On a monthly basis, Contractor shall report to the County the Fees incurred to-date during each Contract Year and the amount of Fees projected to be incurred in the remaining months of the Contract Year. If either Contractor or the County reasonably determine, based upon such monthly report, that the Fees that would be payable are likely to exceed the Maximum Annual Fee prior to the end of the relevant Contract Year, the Parties shall cooperate to make adjustments to the Services, or to the County's requirements in respect of the Services, so that the Fees do not exceed the Maximum Annual Fee. Alternatively, the County may, in its sole discretion, increase the Maximum Annual Fee so that the Maximum Annual Fee is not exceeded; provided, however, that in no event shall the Maximum Annual Fee be increased except by the express written consent of the County's Contracting Officer. The County shall not be obligated to pay Contractor fees in respect of Services in excess of the Maximum Annual Fee.

16.2. Invoices

16.2.1. General

Contractor shall furnish the County Technology Office with the following invoices:

(a) A single invoice for the Monthly Services Charge, calculated in arrears, issued by the fifteenth (15th) day of each month, and payable in accordance with the terms of Schedule 16.1. Each such invoice shall include an itemized accounting of Resource Units incurred during the immediately preceding month.

(b) Invoices shall be accompanied by information and data that support the invoiced Fees. Unless otherwise provided in Schedule 16.1, invoices are payable within sixty (60) days after receipt of invoice correct as to the form agreed by the Parties. The County may dispute any invoice in accordance with the provisions of Section 16.11.

16.2.2. Retroactive Billing

Billing for any Services not reported in writing by Contractor within two (2) monthly reporting periods from the date such Service was provided to the County will not be billable to the County except as otherwise agreed in writing by the County Contracting Officer. Contractor's written report as required by this Section 16.2.2 shall include detailed supporting documentation for that anticipated billing.

16.3. Pricing Audit

Contractor shall, at the County's request, allow auditors designated by the County that are subject to reasonable confidentiality requirements to fully audit Contractor's books and records to the extent necessary to verify any amounts paid or payable by the County hereunder. Contractor shall provide such auditors with full access to such information relating to this Agreement and Contractor's books and records as may be necessary to confirm the accuracy of Contractor's invoices, documents, and other information supporting such invoices, and any pricing adjustment computations. All such audits shall be conducted during business hours, with reasonable advance

notice, and shall include access to proprietary and confidential information to the extent necessary to comply with the provisions of this Section 16.3. If any such audit reveals that Contractor has overcharged the County during the period to which the audit relates, then Contractor shall refund such overcharges to the County through the next monthly invoice and the cost of such audit shall be borne by Contractor. Should Contractor owe County a refund after the final invoice at the conclusion of Disentanglement, Contractor shall issue a draft to County in the amount due within thirty (30) days of the final invoice date.

16.4. Reduction of Payments

If the County terminates as to any of the Service Frameworks described in Schedule 4.3 hereof or terminates any discrete components, deliverables, features, functions, capabilities, tasks, activities, or portions of the Services, pursuant to the terms of Section 4.10 or Section 17.2.1 hereof, then adjustments to the fees for such Services shall go into effect upon the Termination Date for such Terminated Services. No fees pertaining to Terminated Services performed after the Termination Date shall be invoiced to or payable by the County. For the avoidance of doubt, the reduction in fees for any termination of Terminated Services hereunder shall not be calculated by applying Banding to the remaining Services.

16.5. Taxes

All fees payable by the County to Contractor hereunder shall be inclusive of all taxes imposed as of the Effective Date by any domestic or foreign taxing authority in respect of the provision of the Services hereunder, including any sales, use, excise, value-added, services, consumption, or other tax (collectively, "Sales Tax(es)"); provided, however, that the County shall not be responsible for, and such fees shall not include, any personal property taxes on property Contractor owns or leases, for franchise and privilege taxes on Contractor's business, gross receipts taxes to which Contractor is subject, and for income taxes based on Contractor's net income. In the event that a Sales Tax becomes effective after the Effective Date and is assessed on the provision of Services by Contractor that are within scope as of the Effective Date or on Contractor's charges to the County under this Agreement related thereto, however levied or assessed, the County shall be responsible for and pay any such Sales Tax. The Parties agree to cooperate with each other to enable each to more accurately determine its own tax liability and to minimize such liability to the extent legally permissible. Contractor's invoices shall separately state the amounts of any taxes Contractor is properly collecting from the County pursuant to the terms hereof.

16.6. Creation of Possessory Interest

Pursuant to the provisions of Revenue and Taxation Code Section 107.6, Contractor acknowledges that the terms of this Agreement may result in the creation of a possessory interest. If such a possessory interest is vested in Contractor, Contractor may be subjected to the payment of real property taxes levied on such interest. Contractor shall be solely responsible for the payment of any such real property taxes. Contractor shall pay all such taxes when due, and shall not allow any such taxes, assessments, or fees to become a lien against any Location or any improvement thereon; provided, however, that nothing herein shall be deemed to prevent or prohibit Contractor from contesting the validity of any such tax, assessment, or fee in a manner authorized by law.

16.7. Benchmarking

With the County's direction and cooperation, and as part of the Services, Contractor, upon the County's direction, shall participate in benchmarking that shall enable the County to compare pricing and performance set forth in this Agreement with, and to ensure that said pricing and performance are among, the industry's best rates and practices. The County may direct a benchmarking for all of the Services or any component or components of the Services at any time during the Term, and may direct a benchmarking for each component of the Services or all of the Services not more than once during any period of twelve (12) consecutive months after the first year of the Term. County and Contractor shall (i) jointly select the benchmarking firm, (ii) equally share the benchmarking firm's charges, and (iii) jointly enter into a written agreement with the benchmarking firm. Neither Party shall unreasonably delay the signing of such an agreement. Each Party shall have the opportunity to advise the benchmarking firm of any information or factors that it deems relevant to the conduct of the benchmarking, so long as such information is disclosed to the other Party. The benchmarking firm shall provide reports on the benchmarking to both the County and Contractor. If, as a result of any such benchmarking, the benchmarking firm determines that the pricing or performance are not as good, from the County's perspective, as the industry's best rates and practices, then the Parties shall promptly make appropriate adjustments to the relevant prices or performance standards in order that they meet such industry best rates and practices; provided, however, that any adjustments to pricing shall be made in accordance with the methodology set forth in Schedule 16.7.

16.8. Fee Adjustments

Schedule 16.8 specifies certain "Fee Adjustments" that may be imposed in the event of any Failure in respect of Contractor's actual performance of Services as measured against the SLs or Critical Milestones. The Parties acknowledge and agree that these Fee Adjustments are intended to reflect the diminished value of the Services as a result of any such Failure; such Fee Adjustments are not intended to compensate the County for any breach or Default by Contractor under this Agreement, nor to constitute penalties, damages, liquidated damages, or other compensation for any such breach or Default. In no event shall Fee Adjustments be the County's sole and exclusive remedy with respect to any Failure of Contractor. In the event the County recovers damages from Contractor for any breach or Default with respect to any Failure, such damages shall be reduced to the extent of any Fee Reductions previously collected by the County in respect of such Failure.

16.9. Only Payments

The Fees set forth in this Section 16 are the only payments to be made by the County to Contractor under this Agreement. The County shall not pay Contractor any additional fees, assessments, or reimbursements, and Contractor shall be solely responsible for, and shall indemnify the County against, all costs and expenses incurred by Contractor in meeting Contractor's obligations under this Agreement, including labor expenses, Hardware and Software costs, and general business expenses (including travel, meals, and overhead expenses).

16.10. Set-Off

The County may set off against any and all amounts otherwise payable to Contractor pursuant to any of the provisions of this Agreement: (i) any and all amounts owed by Contractor to the County

under the provisions of Section 22; and (ii) other amounts claimed to be owed to the County by Contractor in respect of this Agreement or any other agreement between the Parties. Within twenty (20) days of any set-off by the County, the County shall provide to Contractor a written accounting of such set-off and a written statement of the reasons therefor.

16.11. Disputed Amounts

Subject to and in accordance with the provisions of this Section 16.11, the County may withhold payment of any Contractor invoice (or part thereof) that it in good faith disputes are due or owing. In such case, the County shall, by the applicable due date, pay any amounts then due that are not disputed and provide to Contractor a written explanation of the basis for the dispute as to the disputed amounts. The failure of the County to pay a disputed invoice, or to pay the disputed part of an invoice, shall not constitute a breach or default by the County, so long as the County complies with the provisions of this Section 16.11. In any such event, the Parties shall diligently pursue an expedited resolution of the dispute.

16.12. Most-Favored Customer

Contractor shall evaluate its offerings to U.S. public entity customers upon County's written request ("Notification Date"), which shall not occur more than once per Contract Year. The County's request shall set forth the Framework or Framework Component to be evaluated. If duing the evaluation Contractor determines that the Contractor offers to any new or existing U.S. public entity customer any information and technology outsourcing services of similar scope (including applications and telecommunications) to the Services described in this Agreement and at similar volumes (plus or minus 25% of those provided under this Agreement) and under similar terms and conditions, at a price lower or a discount greater than the price charged or the discounts offered to the County hereunder for any individual Framework or Framework Component, then, on a prospective basis from the Notification Date, defined above, Contractor shall offer such lower price or greater discount to the County in lieu of the price therefor (or discount related thereto) that is reflected in the price set forth in this Agreement for such Framework or Framework Component.

16.13. RESERVED

16.14. Capital Infusion and Depreciation

During each Contract Year, Contractor shall, at its cost and expense, acquire equipment and other items (which include the Purchased Assets in Contract Year 1) for dedicated use in providing the Services. Except for Shared Resources, all such acquisitions shall, for purposes of the County's rights upon Disentanglement pursuant to Section 6.3.6 be capitalized, accounted for, and depreciated by Contractor in accordance with the guidelines set forth in Schedule 16.1, without regard to the actual method of acquisition (i.e., whether by purchase, lease, or other method of financing).

PART VI-GENERAL

17. Term

17.1. Initial Term; Renewals

17.1.1. Initial Term

The period during which Contractor shall be obligated to provide the Services under this Agreement shall commence on the Effective Date (except as otherwise specified herein) and shall end at 11:59.59 PM (Pacific Time) on December 31, 2023 (the "Initial Term"), subject to appropriation by the County of funds for this Agreement for such period.

17.1.2. Notification of Expiration

Contractor shall notify the County of the expiration of the Initial Term, and of any renewal thereof not later than six (6) months before the date on which the Term would expire if not renewed pursuant to Section 17.1.3 or extended pursuant to Section 17.1.4.

17.1.3. Renewal by County

The County may, in its sole discretion and subject to appropriation by the County of funds for this Agreement for such period, extend the Initial Term for up to one renewal period of five (5) years by providing written notice delivered to Contractor at least four (4) months before the end of the Initial Term. Following such notice, the Parties shall negotiate in good faith new fees applicable to Services to be rendered during the upcoming renewal period. While such negotiations are pending, the Contractor shall continue to provide the Services at the then-current Resource Unit Charges until the Parties establish new fees applicable to the Services.

17.1.4. Extensions by County

Notwithstanding anything to the contrary set forth in Sections 17.2 through 17.5, the County may, at its sole option and discretion, upon at least one hundred twenty (120) days' notice to Contractor, extend the effective date of any expiration or termination of the Term or any portion of the Services (e.g., a Service Framework, a category of Service or any portion of such Services) for successive periods of not less than one hundred twenty (120) days each, with such extension periods not to exceed six hundred (600) days in the aggregate for each particular expiration or termination. By way of example only, the County may extend the effective date of any termination of a particular Service Framework for successive periods not to exceed six hundred (600) days in the aggregate and may also extend the effective date of any termination of a different Service Framework for successive periods not to exceed a separately measured six hundred (600) days in the aggregate. Each such extension shall be upon the same terms and conditions in effect immediately prior to such extension. Any adjustments to the Fees applicable to any extension period shall be mutually agreed by the Parties, consistent with the pricing methodology set forth in Schedule 16.1; in the event the Parties are unable to agree on such applicable Fees, the Fees shall be the same Fees as were applicable in the immediately preceding Contract Year or extension period, as the case may be.

17.1.5. Appropriations

To the extent any necessary appropriations are not made in the then-current fiscal year, the County's payment obligations for such fiscal year shall be deemed contingent liabilities only, subject to appropriation in the following fiscal year. In the event that either no funds or insufficient funds are appropriated and budgeted in any fiscal year for payments to be made under this Agreement, the County shall notify Contractor of such occurrence and the Term of this Agreement shall terminate on the earlier of the last day of the fiscal period for which sufficient appropriation was made or whenever the funds appropriated for payment under this Agreement are exhausted.

17.2. Early Termination

17.2.1. For Convenience

The County, after consultation with the Sheriff on any matters related to or affecting CLETS, shall have the right to terminate (i) the Term of this Agreement with regard to the Services; or (ii) any portion of the Services (e.g., a Service Framework, a category of Service or any portion of such Services), for its convenience, by delivering to Contractor a written notice of termination (the "Termination Notice") at least one hundred eighty (180) days before the date or dates then-contemplated by the County in such notice for termination of such Services ("Provisional Termination Date(s)"). In the event the County elects to terminate any Service Framework or category of Service or portion thereof (but not all Services in the aggregate) pursuant to the terms hereof, Contractor shall perform its Disentanglement obligations hereunder to the extent applicable to such Terminated Services. For any termination under this Agreement, in the event the County does not set firm and binding effective date or dates for termination of the Terminated Services (the "Termination Date(s)") in the Termination Notice, the County shall set such Termination Date(s)", via a written notice to Contractor after consultation with the Contractor regarding Disentanglement and/or development of the Disentanglement plan in accordance with Section 6.3.1. The County shall set such Termination Dates in its sole discretion; provided, however, such Termination Date(s) shall not be earlier than the Provisional Termination Date(s) set forth in the Termination Notice, and provided, further, that all Termination Dates shall remain subject to extension pursuant to Section 17.1.4. Any such termination of Terminated Services under this Section shall be effective as of 11:59.59 PM (Pacific Time) on the Termination Date pertaining to such Terminated Services. For the avoidance of doubt, any Remove or other decrease in the quantity of the County's consumption of Services to which the County elects to apply Bands shall not be deemed a termination for convenience under this Section 17.2.1.

17.2.2. Change in Control of Contractor

In the event of a Change in Control of Contractor resulting from a single transaction or series of related transactions, the County shall have the right to terminate the Term of this Agreement with regard to the Services by sending a Termination Notice to Contractor at least ninety (90) days prior to the Provisional Termination Date, provided that the County shall have delivered such notice to Contractor not later than one hundred eighty (180) days following the effective date of such Change in Control. Solely for purposes of this

Section 17.2.2, "Control" shall mean, with respect to any Person, the legal, beneficial, or equitable ownership, direct or indirect, of more than fifty percent (50%) of the aggregate of all voting or equity interests in such Person; "Change in Control" shall mean any change in the legal, beneficial, or equitable ownership, direct or indirect, such that Control of such Person is no longer with the same Person or Persons as on the Effective Date. A Change in Control shall also be deemed to have occurred if, after a single transaction or a series of related transactions, or a restructuring of Contractor, or a transfer or removal of assets from Contractor, or assumption of debt by Contractor, the credit rating of Contractor's senior unsecured indebtedness is "B+" or less as rated by Standard and Poor's; and in such event the County shall have the option, exercisable within one hundred eighty (180) days of the effective date of such deemed Change in Control, to exercise its rights pursuant to this Section 17.2.2. Any such termination pursuant to this Section shall be effective at 11:59.59 PM (Pacific Time) on the Termination Date pertaining to the Terminated Services.

17.3. Termination for Default

The County shall have the right to terminate: (i) the Term of this Agreement with regard to the Services; or (ii) any portion of the Services (e.g., a Service Framework, a category of Service or any portion of such Services), by a Termination Notice delivered to Contractor if Contractor commits a Default. Termination shall be effective at 11:59.59 PM (Pacific Time) on the Termination Date(s) pertaining to such Terminated Services; provided, however, that Contractor shall continue to perform its Disentanglement obligations hereunder until they are fulfilled. No termination pursuant to this Section 17.3 shall be deemed a termination for convenience subject to Section 17.2.1. In the event the County elects to terminate any portion of the Services (e.g., a Service Framework, a category of Service or any portion of such Services) but not all Services in the aggregate, pursuant to the terms hereof, Contractor shall perform its Disentanglement obligations hereunder to the extent applicable to such Terminated Services. Termination shall not constitute the County's exclusive remedy for such Default, and the County shall not be deemed to have waived any of its rights accruing hereunder prior to such Default.

17.4. Termination for Force Majeure Event

If a delay or interruption of performance by Contractor resulting from its experiencing a Force Majeure Event exceeds ten (10) days, despite Contractor's use of its best efforts (that shall not involve the payment of funds that would not be commercially reasonable under the circumstances), the County shall have the right to terminate (i) the Term of this Agreement with regard to the Services; or (ii) any portion of the Services (e.g., a Service Framework, a category of Service or any portion of such Services), all or any portion of the Services (e.g., a Service Framework, a category of Service or any portion of such Services), effective at 11:59.59 PM (Pacific Time) on the Termination Date(s) pertaining to such Terminated Services, by delivering to Contractor a Termination Notice; provided, however, that Contractor shall continue to perform its Disentanglement obligations in respect of such Terminated Services until such obligations are fulfilled.

17.5. Termination by the County

In the event Contractor, any of its Subcontractors, or any of each of their employees is or becomes debarred and declared ineligible, or voluntarily excluded from covered transactions with respect to

all business with the United States government, then the County shall have the right, at its option, to terminate the Term of this Agreement with regard to the Services, effective at 11:59.59 PM (Pacific Time) on the Termination Date pertaining to such Terminated Services, by delivering to Contractor a Termination Notice.

17.6. Effect of Ending of Term

Notwithstanding any provision of this Section 17 to the contrary, the expiration or termination of the Term shall not constitute a termination of this Agreement or any provision hereof that by its nature shall continue in force and effect, including Contractor's obligations with respect to Disentanglement.

17.7. No Termination by Contractor

Contractor may not, for any reason whatsoever, terminate the Term prior to its expiration, terminate this Agreement, or otherwise repudiate this Agreement or refuse to perform its obligations hereunder.

18. Remedies; Limitations of Liability

18.1. Remedies Cumulative

Except as otherwise expressly limited in Section 18.2, below, or elsewhere in this Agreement, the remedies provided in this Section and elsewhere in this Agreement are neither exclusive nor mutually exclusive, and the Parties shall be entitled to resort to any and all such remedies, and any other remedy or remedies available at law or in equity, by statute or otherwise, individually or in any combination thereof. No delay in exercising or failure to exercise any right or remedy shall operate as a waiver thereof except where specifically provided herein.

18.2. Limitation of Liability and Disclaimers

Subject to the express provisions and limitations of this Section 18.2, the Parties intend that each Party shall be liable to the other Party for all damages incurred as a result of the breaching Party's failure to perform its obligations.

(a) EXCEPT AS OTHERWISE EXPRESSLY PROVIDED BELOW, THE AGGREGATE CUMULATIVE MONETARY LIABILITY OF THE COUNTY HEREUNDER FOR ALL CLAIMS ARISING UNDER OR RELATING TO THIS AGREEMENT, NOTWITHSTANDING THE FORM (e.g., CONTRACT, TORT, OR OTHERWISE) IN WHICH ANY ACTION IS BROUGHT, SHALL BE LIMITED TO TWO HUNDRED MILLION DOLLARS ($200,000,000.00). THE FOREGOING LIMITATIONS UPON THE COUNTY'S LIABILITY SHALL NOT APPLY TO: (i) LOSSES SUBJECT TO INDEMNIFICATION BY THE COUNTY; (ii) LOSSES ARISING FROM THE COUNTY'S FAILURE TO COMPLY WITH SECTION 12.10; OR (iii) LOSSES ARISING OUT OF THE WILLFUL MISCONDUCT OR GROSS NEGLIGENCE OF THE COUNTY.

(b) EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS SECTION 18.2, THE AGGREGATE CUMULATIVE MONETARY LIABILITY OF CONTRACTOR HEREUNDER FOR ALL DAMAGES ARISING UNDER OR RELATING TO THIS AGREEMENT, NOTWITHSTANDING THE FORM

(e.g., CONTRACT, TORT, OR OTHERWISE) IN WHICH ANY ACTION IS BROUGHT, SHALL BE LIMITED TO TWO HUNDRED FIFTY MILLION DOLLARS ($250,000,000.00); PROVIDED, HOWEVER, THAT TO THE EXTENT THE DAMAGES ARE DESCRIBED IN SECTION 18.2(c), IN LIEU OF THE FOREGOING LIMITATION, THE AGGREGATE CUMULATIVE MONETARY LIABILITY SHALL NOT EXCEED ONE HUNDRED THIRTY PERCENT (130%) OF THE FOREGOING LIMITATION. THE FOREGOING LIMITATION UPON THE TYPES AND AMOUNTS OF CONTRACTOR'S LIABILITY SHALL NOT APPLY TO: (A) LOSSES ARISING FROM CONTRACTOR'S BREACHES OF ITS TRANSITION OBLIGATIONS IN SECTIONS 2 AND 3 (INCLUDING BREACHES OF THE TRANSITION PLAN); (B) LOSSES SUBJECT TO INDEMNIFICATION BY CONTRACTOR; (C) LOSSES ARISING FROM CONTRACTOR'S FAILURE TO COMPLY WITH THE PROVISIONS OF SECTION 12 OR 21.1.2.3; (D) LOSSES ARISING FROM CONTRACTOR'S REPUDIATION OF, OR UNEXCUSED REFUSAL TO PERFORM, THIS AGREEMENT OR ITS FAILURE OR REFUSAL TO CONTINUE SERVICES IN VIOLATION OF SECTIONS 17.7 OR 23.3; (E) LOSSES ARISING FROM CONTRACTOR'S WITHHOLDING OF DATA IN VIOLATION OF SECTION 15.8; (F) LOSSES ARISING OUT OF THE WILLFUL MISCONDUCT OR GROSS NEGLIGENCE OF CONTRACTOR; (G) LOSSES ARISING FROM CONTRACTOR'S FAILURE TO PERFORM DISENTANGLEMENT IN ACCORDANCE WITH SECTION 6 AND THE DISENTANGLEMENT PLAN; AND (H) COST AND EXPENSES OF RESTORING ANY ALTERED, LOST OR STOLEN COUNTY DATA.

(c) CONTRACTOR ACKNOWLEDGES AND AGREES THAT THE TYPES OF DAMAGES THAT THE COUNTY MAY RECOVER FROM CONTRACTOR SHALL INCLUDE ALL ADDITIONAL INTERNAL AND EXTERNAL COSTS AND EXPENSES PAID OR INCURRED BY THE COUNTY AS A DIRECT RESULT OF ANY FAILURE BY CONTRACTOR TO PERFORM ITS OBLIGATIONS HEREUNDER, INCLUDING ANY ADDITIONAL COSTS INCURRED BY THE COUNTY TO OBTAIN REPLACEMENT SERVICES COMPLYING WITH THE TERMS HEREOF.

(d) EXCEPT TO THE EXTENT ANY OF THE LOSSES DESCRIBED IN (1) CLAUSES (i) - (iii) OF SUBSECTION (a), (2) CLAUSES (A), – (H) OF SUBSECTION (b), OR (3) SUBSECTION (c) MAY BE DEEMED TO BE SUCH DAMAGES, NEITHER PARTY SHALL BE LIABLE FOR CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE, INDIRECT, OR INCIDENTAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE FORM IN WHICH ANY ACTION IS BROUGHT.

(e) NOTWITHSTANDING ANY OTHER PROVISION OF THIS SECTION 18.2, CONTRACTOR'S LIABILITY AND CONTRACTOR'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 22.3, NOTWITHSTANDING THE FORM OF ACTION (e.g., CONTRACT, TORT, OR OTHERWISE), IS LIMITED BY THIS SECTION 18.2(e) IF SUCH LIABILITY IS CAUSED BY THE THIRD PARTY LISTED ON SCHEDULE 18.2 AND DIRECTLY ARISES OUT OF

THAT THIRD PARTY'S PERFORMANCE UNDER THE CONTRACTOR'S LIABILITY SHALL BE LIMITED BASED ON THE VALUE OF THE THIRD PARTY CONTRACT OR SUBCONTRACT AS SET FORTH IN THE TABLE BELOW:

Contract/Subcontract Value	Maximum Liability for Contractor
Under $1,000,000	$10,000,000
$1,000,000 - $10,000,000	$20,000,000
Over $10,000,000	Two times the value of the subcontract up to $250,000,000

THE FOREGOING LIMITATION ON CONTRACTOR'S LIABILITY ARISING OUT OF SECTION 22.3 SHALL NOT APPLY TO THE EXTENT THE DAMAGES ARISE FROM CONTRACTOR'S BREACHES OF THE THIRD PARTY CONTRACT.

THE CONTRACTOR'S LIABILITY, TO THE EXTENT ARISING OUT OF ALL OTHER THIRD PARTY CONTRACTS, AND ANY INDEMNIFICATION OBLIGATIONS UNDER SECTION 22.3 FOR SUCH THIRD PARTY CONTRACTS, SHALL BE LIMITED AS SET FORTH IN SECTION 18.2(b) (EXCEPT FOR SECTION 18.2(b)(B)).

18.3. Force Majeure Events

Except as expressly provided in this Agreement, if a Force Majeure Event is the material cause of a Party's failure to perform any of its obligations hereunder, such obligations, after notification by such Party to the other Party, shall be deemed suspended to the extent such obligations are directly affected by such Force Majeure Event, until the Force Majeure Event has ended and a reasonable period of time for overcoming the effects thereof has passed; provided, however, that if a Force Majeure Event results in Contractor being unable to perform during any period any or all of the Services in accordance with the terms hereof, the County shall: (i) not be required to pay for any such Services that Contractor is unable to perform; (ii) be entitled, without the payment of the fees described in Section 17.2.1, to engage an alternate provider, on an interim basis, to perform the Services that Contractor is unable to perform as a result of such Force Majeure Event; (iii) be entitled to a share of Contractor's resources devoted to returning Contractor to full performance of all Services hereunder, that is equal to or greater than the share of such resources that Contractor allocates to other of its customers with whom it has agreements that are similar to this Agreement; and (iv) have the right to terminate this Agreement in accordance with the terms of Section 17.4 hereof. Both Parties shall use their best efforts to minimize delays that occur due to a Force Majeure Event. Notwithstanding the above, Contractor shall in no event be excused from those obligations not directly affected by a Force Majeure Event, and if the Force Majeure Event is caused by Contractor's failure to comply with any of its obligations under this Agreement or by Contractor's negligence or omission, there shall be no relief from any of its obligations under this Agreement. In addition, notwithstanding any of the above, Contractor shall be obligated to provide the disaster recovery services as set forth in Schedule 4.3 at all times without regard to any Force Majeure Event.

19. Insurance

Without limiting Contractor's indemnification obligations to County, Contractor shall provide at its sole expense and maintain for the duration of this Agreement, or as may be further required herein, insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the Services hereunder and the results of the Services by the Contractor, his agents, representatives, employees or Subcontractors. Contractor's insurance requirements are set for the in Schedule 19.

20. Legal Compliance

20.1. Compliance with All Laws and Regulations

Contractor shall at all times perform its obligations hereunder in compliance with all applicable federal, State, and County laws and regulations (including facility and professional licensing and/or certification laws) of all applicable jurisdictions, and in such a manner as not to cause the County to be in violation of any applicable laws or regulations, including any applicable requirements of any federal, State of California or other state or the District of Columbia and in which Services are provided, or County authority regulating County Data, Public Record Data, privacy, wages and hours of employment, health, sanitation, safety, the environment, or telecommunications. Contractor shall maintain and keep in effect any and all licenses, permits, notices and certifications as are required. Additionally, Contractor shall comply with the County's Affirmative Action Program for Vendors as set forth in Article IIIk (commencing at Section 84) of the San Diego County Administrative Code, which program is incorporated herein by reference. A copy of such Program shall be provided to Contractor upon its request. Nothing in this Agreement shall be deemed to transfer to Contractor any of the County's responsibilities or obligations related to the use, management, or disbursement of any funds the County receives from the federal or the State government. No provision of this Agreement, including any Service Request, shall have any force or effect if it would cause a violation of any federal or State law, ordinance, statute, rule, regulation, or order, or would require any consent or approval to prevent any such violation.

20.2. Contractor Permits and License

Contractor shall obtain and maintain, and shall cause its Subcontractors to obtain and maintain, at no cost to the County, all approvals, permissions, permits, licenses, and other forms of documentation required in order to comply with all existing foreign or domestic statutes, ordinances, and regulations, or other laws, that may be applicable to performance of Services hereunder. The County reserves the right to reasonably request and review all such applications, permits, and licenses prior to the commencement of any Services hereunder. If requested, the County shall cooperate with Contractor, at Contractor's cost and expense, to obtain any such approvals, permits, and licenses.

20.3. Americans with Disabilities Act

Contractor shall not discriminate against qualified people with disabilities in employment, public services, transportation, public accommodations and telecommunications services in compliance with the Americans with Disabilities Act ("ADA") and California Administrative Code Title 24.

20.4. Equal Opportunity

Contractor shall comply with the provisions of Title VII of the Civil Rights Act of 1964 in that it will not discriminate against any individual with respect to his or her compensation, terms, conditions, or privileges of employment nor shall Contractor discriminate in any way that would deprive or intend to deprive any individual of employment opportunities or otherwise adversely affect his or her status as an employee because of such individual's race, color, religion, sex, national origin, age, handicap, medical condition, sexual orientation or marital status.

20.5. Non-Discrimination

Contractor shall ensure that Services and facilities are provided without regard to ethnic group identification, race, color, nation origin, creed, religion, age, sex, or physical or mental disability in accordance with Title IX of the Education Amendments of 1972; Title VII of the Civil Rights Act of 1964 (42 U.S.C. 2000-d), the Age Discrimination of 1975 (42 U.S.C. 6101), Article 9.5, Chapter 1, Part 1, Division 2, Title 2 (Section 11135, et seq) of the California Government Code, and Title 9, Chapter 4, Subchapter 6 (Section 10800, et seq.) of the CCR.

20.6. AIDS Discrimination

Contractor shall not deny any person the full and equal enjoyment of, or impose less disadvantageous terms, or restrict the availability of, the use of any Location or participation in any County funded or supported service or program on the grounds that such person has Acquired Immune Deficiency Syndrome, AIDS-related complex (ARC), or AIDS-related status (ARS), as those terms are defined in Chapter 1, Section 32.803, San Diego County Code of Regulatory Ordinances.

20.7. Contractor Certification

Contractor represents and warrants that Contractor has not been convicted of bribing or attempting to bribe an officer or employee of the County, nor has Contractor made an admission of guilt of such conduct that is a matter of record.

20.8. Board of Supervisors' Policies

Contractor represents that it is familiar, and shall use its best efforts to comply, with the following policies of the Board of Supervisors:

(a) Policy B-67, which encourages the County's contractors to offer products made with recycled materials, reusable products, and products designed to be recycled to the County in response to the County's requirements; and

(b) Policies B-53 and B-39a, which encourage the participation of small and disabled veterans' business enterprises in County procurements.

20.9. Debarment and Suspension

20.9.1. Contractor Certification

As a sub-grantee of federal funds under this Agreement, Contractor certifies that it, and its Affiliates and Subcontractors, and its and their employees:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;

(b) have not, within the three (3) year period preceding this Agreement, been convicted of or had a civil judgment rendered against any of them for: the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction; violation of federal or state anti-trust statutes; or the commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(c) are not presently indicted or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses described in paragraph (b); and

(d) have disclosed any instances in which, within the three (3) year period preceding this Agreement, had one or more public transaction (federal, State, or local) terminated for cause or default.

20.10. Hazardous Materials

Contractor shall be responsible for compliance with all Environmental Laws and all other laws, rules, regulations, and requirements regarding Hazardous Materials, health and safety, notices, and training. Contractor agrees that it will not store any Hazardous Materials at any Location for periods in excess of ninety (90) days or in violation of the applicable site storage limitations imposed by Environmental Law. Contractor agrees to take, at its expense, all actions necessary to protect third parties, including, without limitation, employees and agents of the County, from any exposure to Hazardous Materials generated or utilized in its performance under this Agreement. Contractor agrees to report to the appropriate governmental agencies all discharges, releases, and spills of Hazardous Materials that are required to be reported by any Environmental Law and to immediately notify the County of same. Contractor shall not be liable to the County for the County's failure to comply with, or violation of, any Environmental Law.

20.11. Prohibited Contracts

Under Section 67 of the San Diego County Administrative Code, Contractor certifies that the provisions of Section 67 have not been violated, and that Contractor is not, and will not subcontract with, any of the following:

(a) Persons employed by the County or by any public agency for which the Board of Supervisors is the governing body;

(b) Profit-making firms or businesses in which employees described in sub-Section (a) serve as officers, principals, partners, or major shareholders;

(c) Persons who, within the immediately-preceding twelve (12) months, came within the provisions of paragraphs (a) or (b) and who (i) were employed in positions of substantial responsibility in the area of service to be performed under this Agreement, or (ii) participated in any way in developing this Agreement or its service specifications; and

(d) Profit-making firms or businesses in which the former employees described in paragraph (c) serve as officers, principals, partners, or major shareholders.

20.12. Political Activities Prohibited

None of the funds, provided directly or indirectly, under this Agreement shall be used for any political activities or to further the election or defeat of any candidate for public office. Contractor shall not utilize or allow its name to be utilized in any endorsement of any candidate for elected office. Neither the contract nor any funds provided thereunder shall be utilized in support of any partisan political activities, or activities for or against the election of a candidate for an elected office.

20.13. Lobbying

Contractor agrees to comply with the lobbying ordinances of the County and to assure that its officers and employees comply before any appearance before the County Board of Supervisors. None of the funds provided under this Agreement shall be used for publicity or propaganda purposes designed to support or defeat any legislation pending before state or federal legislatures or the Board of Supervisors of the County.

20.14. Religious Activity Prohibited

There shall be no religious worship, instructions or proselytization as part of or in connection with the performance of this Agreement.

20.15. Drug and Alcohol-Free Workplace

The County, in recognition of individual rights to work in a safe, healthful and productive work place, has adopted a requirement for a drug and alcohol free work place, County of San Diego Drug and Alcohol Use Policy C-25. This policy provides that all County-employed contractors and Contractor employees shall assist in meeting this requirement.

20.15.1. As a material condition of this Contract, the Contractor agrees that the Contractor and the Contractor employees, while performing service for the County, on County property, or while using County equipment:

(a) Shall not be in any way impaired because of being under the influence of alcohol or a drug.

(b) Shall not possess an open container of alcohol or consume alcohol or possess or be under the influence of an illegal drug.

(c) Shall not sell, offer, or provide alcohol or a drug to another person; provided, however, that the foregoing restriction shall not be applicable to a Contractor or Contractor employee who as part of the performance of normal job duties and responsibilities prescribes or administers medically prescribed drugs.

20.15.2. Contractor shall inform all employees who are performing service for the County on County property or using County equipment of the County objective of a safe, healthful and productive work place and the prohibition of drug or alcohol use or impairment from same while performing such service for the County.

20.15.3. The County may terminate for default or breach this Agreement, and any other contract the Contractor has with the County, if the Contractor, or Contractor employees are determined by the Contracting Officer not to be in compliance with the conditions listed in this Section 20.15.

20.16. Cartwright Act.

Following receipt of final payment under the Agreement, Contractor assigns to the County all rights, title and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright act (Chapter 1) (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the Contractor for sale to the County under this Agreement.

20.17. Zero Tolerance for Fraudulent Conduct In County Services

Contractor shall comply with County of San Diego Board of Supervisors Policy A-120 "Zero Tolerance for Fraudulent Conduct in County Services." There shall be "Zero Tolerance" for fraud committed by contractors in the administration of County programs and the provision of County services. Upon proven instances of fraud committed by independent contractors in connection with their performance under the contract, said contract shall be terminated.

20.18. Family-Centered Practice, Board of Supervisors Policy E-13

Contractor shall comply with County of San Diego Board of Supervisors Policy E-13, "Family-Centered Practice." Family-centered practice addresses the needs of the whole family and is intended to promote and support community and family involvement to ensure safe and healthy environments for children.

20.19. Interlocking Directorate

In recognition of County Policy A-79, not-for-profit Contractors shall not subcontract with related for-profit subcontractors for which an interlocking relationship exist unless specifically authorized in writing by the Board of Supervisors.

20.20. Zero Tolerance in Coaching Medi-Cal or Welfare Clients (Including Undocumented Immigrants)

The County of San Diego in recognition of its unique geographical location and the utilization of Welfare and Medi-Cal system by foreign nationals who are not legal constituents of this county or country, has adopted a Zero Tolerance policy and shall aggressively prosecute employees and contractors who coach Medi Cal or Welfare clients (including undocumented immigrants), to obtain services for which they are not otherwise entitled.

As a material condition of this Agreement, Contractor agrees that the Contractor and Contractor's employees, while performing service for the County, on County property or while using County equipment shall not:

(a) in any way coach, instruct, advise, or guide any Medi-Cal or Welfare clients or prospective clients who are undocumented immigrants on ways to obtain or qualify for Medi-Cal assistance, for which they are not otherwise entitled.

(b) support or provide funds to any organization engaged directly or indirectly in advising undocumented immigrants on ways to obtain or qualify for Medi-Cal assistance, for which they are not otherwise entitled.

Contractor shall inform all Subcontractors and employees that are performing service for the County on County property or using County equipment of County's Zero Tolerance Policy as referenced herein.

County may terminate for default or breach this Agreement and any other contract Contractor has with County, if Contractor or Contractor employees are determined not to be in compliance with the conditions stated herein.

20.21. Equal Employment Opportunity

The following applies only to "federally assisted construction contracts" as defined in 41 C.F.R. § 60-1.3:

During the performance of this Agreement, the Contractor agrees as follows:

(a) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

(b) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(c) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to

individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

(d) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(e) The Contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(f) The Contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(g) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this Agreement or with any of the said rules, regulations, or orders, this Agreement may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(h) The Contractor will include the portion of the sentence immediately preceding paragraph (a) and the provisions of paragraphs (a) through (h) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance: Provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States. The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: Provided, That if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the Agreement.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance. The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

20.22. Contracting With Small and Minority Businesses, Women's Business Enterprises, and Labor Surplus Area Firms

Contractor shall, in accordance with 2 CFR 200.321 - Contracting with small and minority businesses, women's business enterprises, and labor surplus area firms, take affirmative steps to include minority business, women's business enterprises, and labor surplus area firm by:

(a) Placing qualified small and minority businesses and women's business enterprises on solicitation lists;

(b) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;

(c) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;

(d) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises; and

(e) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce.

20.23. Davis-Bacon Act

The following only applies to construction contracts in excess of $2,000:

(a) All transactions regarding this Agreement shall be done in compliance with the Davis-Bacon Act (40 U.S.C. 3141- 3144, and 3146-3148) and the requirements of 29 C.F.R. pt. 5 as may be applicable. The Contractor shall comply with 40 U.S.C. 3141-3144, and 3146-3148 and the requirements of 29 C.F.R. pt. 5 as applicable.

(b) Contractors are required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.

(c) Additionally, contractors are required to pay wages not less than once a week.

20.24. Copeland Anti-Kickback Act

The following only applies to construction or repair contracts in excess of $2,000 in situations where the Davis-Bacon Act also applies:

(a) Contractor. The Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into this Agreement.

(b) Subcontracts. The Contractor or subcontractor shall insert in any subcontracts the clause above and such other clauses as FEMA may by appropriate instructions require, and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime Contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses.

(c) Breach. A breach of the contract clauses above may be grounds for termination of the Agreement, and for debarment as a Contractor and subcontractor as provided in 29 C.F.R. § 5.12.

20.25. Contract Work Hours and Safety Standards Act

The following only applies to contracts in excess of $100,000 that involve the employment of mechanics or laborers. It is applicable to construction work. These requirements do not apply to the purchase of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence:

(a) Overtime requirements. No Contractor or subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

(b) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (a) of this section the Contractor and any subcontractor responsible therefor shall be liable for the unpaid wages. In

addition, such Contractor and subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (a) of this section, in the sum of $26 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (a) of this section.

(c) Withholding for unpaid wages and liquidated damages. The County shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the Contractor or subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime Contractor, such sums as may be determined to be necessary to satisfy any liabilities of such Contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (b) of this section.

(d) Subcontracts. The Contractor or subcontractor shall insert in any subcontracts the clauses set forth in paragraph (a) through (d) of this section and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime Contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (a) through (d) of this section.

20.26. Clean Air Act and the Federal Water Pollution Control Act

This provision only applies to contracts in excess of $150,000:

(a) The Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

(b) The Contractor agrees to report each violation to the County and understands and agrees that the County will, in turn, report each violation as required to assure notification to the appropriate federal agency, and the appropriate Environmental Protection Agency Regional Office.

(c) The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA, HUD, or other federal agency.

(d) The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

20.27. Debarment and Suspension

(a) This Agreement is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, the Contractor is required to verify that none of the Contractor's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(b) The Contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(c) This certification is a material representation of fact relied upon by County. If it is later determined that the Contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to County, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

(d) The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

20.28. Byrd Anti-Lobbying Amendment

(a) Contractors who apply or bid for an award of $100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the awarding agency.

(b) If applicable, Contractor must sign and submit to the County the following certification:

APPENDIX A, 44 C.F.R. PART 18 – CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the

extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

The Contractor, _____, certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. Chap. 38, Administrative Remedies for False Claims and Statements, apply to this certification and disclosure, if any.

_____

Signature of Contractor's Authorized Official

_____

Name and Title of Contractor's Authorized Official

_____

Date

20.29. Procurement of Recovered Materials

(a) In the performance of this Agreement, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired—

- Competitively within a timeframe providing for compliance with the contract performance schedule;
- Meeting contract performance requirements; or
- At a reasonable price.

(b) Information about this requirement, along with the list of EPA-designated items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensiveprocurement-guideline-cpg-program.

(c) The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act."

20.30. Access to Records

The following access to records requirements apply to this Agreement:

(a) The Contractor agrees to provide County, the State of California, the Federal Agency Secretary or Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this Agreement for the purposes of making audits, examinations, excerpts, and transcriptions.

(b) The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

(c) The Contractor agrees to provide the Federal Agency or Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the Agreement.

(d) In compliance with the Disaster Recovery Act of 2018, the County and the Contractor acknowledge and agree that no language in this Agreement is intended to prohibit audits or internal reviews by the Federal Agency or Administrator or the Comptroller General of the United States.

20.31. Rights to Inventions Made Under a Contract or Agreement

If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the recipient or sub-recipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or sub-recipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

20.32. DHS Seal, Logo, and Flags

The Contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.

20.33. Compliance With Federal Law, Regulations, and Executive Orders

This is an acknowledgement that federal financial assistance may be used to fund all or a portion of the Agreement. The Contractor will comply with all applicable Federal law, regulations, executive orders, federal agency policies, procedures, and directives.

20.34. No Obligation By Federal Government

The Federal Government is not a party to this Agreement and is not subject to any obligations or liabilities to the County, Contractor, or any other party pertaining to any matter resulting from the Agreement.

20.35. Program Fraud and False or Fraudulent Statements or Related Acts

The Contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the Contractor's actions pertaining to this Agreement.

20.36. Domestic Preferences

In accordance with 2 CFR part 200.322, as appropriate and to the extent consistent with law, Contractor shall, to the greatest extent practicable, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products).

20.36.1. "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, must occur in the United States.

20.36.2. "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based

20.37. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

In accordance with 2 CFR part 200.216, Contractor and its subcontractors are prohibited from expending funds under this Agreement to:

20.37.1. Procure or obtain;

20.37.2. Extend or renew a contract to procure or obtain; or

20.37.3. Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

20.37.3.1. For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or

20.37.3.2. Telecommunications or video surveillance services provided by such entities or using such equipment.

20.37.3.3. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or

otherwise connected to, the government of a covered foreign country

21. Representations and Warranties

21.1. Contractor Representations, Warranties, and Related Covenants

21.1.1. Performance of the Services

Contractor represents and warrants that it is capable in all respects of providing and shall provide all Services in accordance with this Agreement. Contractor further represents and warrants that: (i) all Services provided under this Agreement shall be provided in a timely, professional, and workmanlike manner consistent with the highest standards of quality and integrity and shall meet the performance standards required under this Agreement; and (ii) no amendment to this Agreement or additional cost or expense shall be required by Contractor in order for it to be able to perform the Services.

21.1.2. Conflict of Interest

Contractor represents, warrants, and agrees that:

21.1.2.1. No Financial Interest

Neither Contractor or any of its Affiliates, nor any employee of either, has, shall have, or shall acquire, any contractual, financial, business, or other interest, direct or indirect, that would conflict in any manner or degree with Contractor's performance of its duties and responsibilities to the County under this Agreement or otherwise create an appearance of impropriety with respect to the award or performance of this Agreement; and Contractor shall promptly inform the County of any such interest that may be incompatible with the interests of the County;

21.1.2.2. No Abuse of Authority for Financial Gain

Neither Contractor or any of its Affiliates, nor any employee of either, has used or shall use the authority provided or to be provided under this Agreement to obtain financial gain for Contractor, or any such Affiliate or employee, or a member of the immediate family of any such employee;

21.1.2.3. No Use of Information for Financial Gain

Neither Contractor or any of its Affiliates, nor any employee of either, has used or shall use any County Confidential Information acquired in the award or performance of the Agreement to obtain financial gain for Contractor, or any such Affiliate or employee, or a member of the immediate family of any such employee;

21.1.2.4. Independent Judgment

Neither Contractor or any of its Affiliates, nor any employee of either, has accepted or shall accept another County contract that would impair the independent judgment of Contractor in the performance of this Agreement;

21.1.2.5. No Influence

Neither Contractor or any of its Affiliates, nor any employee of either, has accepted or shall accept anything of value based on an understanding that the actions of Contractor or any such Affiliate or employee on behalf of the County would be influenced; and Contractor shall not attempt to influence any County employee by the direct or indirect offer of anything of value;

21.1.2.6. No Payment Tied to Award

Neither Contractor or any of its Affiliates, nor any employee of either, has paid or agreed to pay any Person, other than bona fide employees working solely for Contractor or such Affiliate or its Subcontractors, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Agreement; and

21.1.2.7. Independent Prices, Terms and Conditions

The prices, terms and conditions presented in the Responses were arrived at independently, without consultation, communication, or agreement with any other proposer for the purpose of restricting competition; the prices, terms and conditions quoted were not knowingly disclosed by Contractor to any other proposer; and no attempt was made by Contractor to induce any other Person to submit or not to submit a proposal for the purpose of restricting competition.

21.1.3. Financial Condition and Information

21.1.3.1. Financial Condition

Contractor represents and warrants that it has, and promises that it shall maintain throughout the Term, a financial condition commensurate with the requirements of this Agreement. If, during the Term, Contractor experiences a change in its financial condition that may adversely affect its ability to perform under this Agreement, then it shall immediately notify the County of such change.

21.1.3.2. Accuracy of Information

Contractor represents and warrants that all financial statements, reports, and other information furnished by Contractor to the County in connection with the award of this Agreement fairly and accurately represent the business, properties, financial condition, and results of operations of Contractor as of the respective dates, or for the respective periods, covered by such financial statements, reports, or other information. Since the respective dates or periods covered by such financial statements, reports, or other information, there has been no

material adverse change in the business, properties, financial condition, or results of operations of Contractor.

21.1.4. Litigation and Service of Process

Contractor represents that there is no pending or anticipated civil or criminal litigation in any judicial or administrative forum that involves Contractor or any of its Affiliates or Subcontractors that may adversely affect Contractor's ability to perform its obligations under this Agreement. Contractor shall notify the County, within fifteen (15) days after its occurrence, of any such pending or anticipated civil or criminal litigation. Contractor shall notify the County, within twenty-four (24) hours in the event process is served on Contractor in connection with this Agreement, including any subpoena of Contractor's records, and shall send a written notice of the service together with a copy of the same to the County within thirty-six (36) hours of such service. If Contractor fails to notify the County of any such pending or anticipated civil or criminal litigation or service of process within such times, the County may terminate this Agreement pursuant to the provisions of Section 17.3.

21.1.5. Proprietary Rights Infringement

Contractor represents and warrants that at no time during the Term shall the use of any services, techniques, materials or products provided or used by Contractor, or its Affiliates or Subcontractors, in performing the Services (including, but not limited to the Contractor Works, Third-Party Works and Work Product), or the use thereof by the County, infringe upon any third-party's patent, trademark, copyright, or other intellectual-property right, nor shall Contractor misappropriate any trade secrets or make use of any misappropriated trade secrets in the performance of Services hereunder.

21.1.6. Legal and Corporate Authority

Contractor represents and warrants that: (i) it is a Limited Liability Company, and is qualified and registered to transact business in all locations where the performance of its obligations hereunder would require such qualification; (ii) it has all necessary rights, powers, and authority to enter into and perform this Agreement, and the execution, delivery, and performance of this Agreement by Contractor has been duly authorized by all necessary corporate action; (iii) the execution and performance of this Agreement by Contractor shall not violate any law, statute, or regulation and shall not breach any agreement, covenant, court order, judgment, or decree to which Contractor is a party or by which it is bound; (iv) it has, and promises that it shall maintain in effect, all governmental licenses and permits necessary for it to provide the Services contemplated by this Agreement; and (v) it owns or leases and promises that it shall own or lease, free and clear of all liens and encumbrances, other than lessors' interests, or security interests of Contractor's lenders, all right, title, and interest in and to the tangible property and technology and the like that Contractor intends to use or uses to provide such Services and in and to the related patent, copyright, trademark, and other proprietary rights, or has received appropriate licenses, leases, or other rights from third parties to permit such use.

21.1.7. Violations

Contractor represents and warrants that it is not, and promises that it shall not be, in violation of any laws, ordinances, statutes, rules, regulations, or orders of governmental or regulatory authorities to which it is subject, and has not failed, and shall not fail, to obtain any licenses, permits, franchises, or other governmental authorizations necessary for the ownership of its properties or the conduct of its business, which violation or failure, either individually or in the aggregate, might adversely affect its business, properties, or financial condition, the consummation of the transactions contemplated by this Agreement, or the performance of its obligations hereunder.

21.1.8. Information Furnished to the County

Contractor represents and warrants that all written information furnished to the County prior to the Effective Date by or on behalf of Contractor in connection with this Agreement is true, accurate, and complete, and contains no untrue statement of a material fact or omits any material fact necessary to make such information not misleading.

21.1.9. Previous Participation in Outsourcing Process

Contractor represents and warrants that neither it, nor any of its Affiliates or Subcontractors that will provide Services at any time under this Agreement, directly or indirectly participated in any of the following activities on behalf of the County with respect to this Agreement: (i) preparation of any Request for Proposal; (ii) development of bid specifications or proposal requirements; (iii) evaluation of bids or proposals; or (iv) negotiations with potential prime contractors.

21.1.10. Previous Contracts

Contractor represents and warrants that neither it, nor any of its Affiliates or Subcontractors, is in default or breach of any other contract or agreement related to information systems or telecommunication system facilities, equipment, or services that it or they may have with the County or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that neither it, nor any of its Affiliates or Subcontractors, has been a party to any contract for information system or telecommunication system facilities, equipment, or services with the County or any of its departments that was finally terminated by the County or such department within the previous five (5) years for the reason that Contractor or such Person failed to perform or otherwise breached an obligation of such contract. Contractor promises that it shall notify the County, within five (5) days of its occurrence, if it, or any of its Affiliates or Subcontractors, is a party to any contract for information system or telecommunication system facilities, equipment, or services with any federal, State, County, or municipal body, or any agency thereof, which contract is finally terminated by such body for the reason that Contractor or such Person failed to perform or otherwise breached an obligation of such contract. If the termination of any such contract is being contested as of the Signing Date in an arbitration or judicial proceeding, the termination shall not be final until the conclusion of such arbitration or judicial proceeding. If the factfinder determines, or a settlement stipulates, that Contractor or such Person failed to perform or otherwise

breached an obligation of such contract, County may terminate this Agreement at the County's sole discretion without County incurring any additional charges whatsoever for such termination.

21.2. County's Representations, Warranties, and Covenants

21.2.1. Legal Authority

The County represents and warrants that it has all necessary rights, powers, and authority to enter into and perform this Agreement; that the execution, delivery, and performance of this Agreement by the County have been duly authorized by all necessary action of the County's Board of Supervisors.

21.2.2. Disclaimer

The County does not make any representation or warranty, express or implied, with respect to the Services or any component thereof, or the skills, capabilities, or medical or other condition of any Transitioned Employees. All hardware, software, networks, and other IT- and telecommunications-related assets made available or conveyed by the County and/or Legacy Provider to Contractor under this Agreement are made available or conveyed to Contractor "AS IS, WHERE IS" and there are no warranties of any kind with respect to the condition, capabilities, or other attributes of such items, except as otherwise expressly stated in this Agreement.

21.3. Warranty Disclaimer

EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, THERE ARE NO EXPRESS WARRANTIES BY EITHER PARTY. THERE ARE NO IMPLIED WARRANTIES OR CONDITIONS, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR OTHERWISE ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE.

21.4. Waiver

Having had reasonable access to pertinent County information and County personnel, and a reasonable time within which to perform due diligence investigation, and having taken into account the possibility that the information it has received might possibly be incorrect or incomplete, Contractor hereby waives and releases any and all claims that it now has or hereafter may have against the County based upon the inaccuracy or incompleteness of the information it has received from, or with regard to, the County. Further, Contractor consents and agrees that it shall not seek any judicial rescission, cancellation, termination, reformation, or modification of this Agreement or any provision hereof, nor any adjustment in the fees to be paid for the Services, based upon any such inaccuracy or incompleteness of information except where such information was intentionally withheld or intentionally misrepresented.

22. Indemnification

22.1. Technology

Contractor shall indemnify, defend, and hold the County Indemnitees harmless from and against any and all Losses in connection with any and all claims or demands brought by any third-party

against any of them for any actual or alleged infringement of any patent, trademark, copyright, or other proprietary right, including misappropriation of trade secrets, (i) based upon technology or intellectual property used by Contractor (including but not limited to Contractor Works, Third-Party Works and Work Product) in providing the Services, or (ii) arising from the County's use or receipt of the Services (including but not limited to the use or receipt of the Contractor Works, Third-Party Works and Work Product or the exercise of any Intellectual Property Rights therein), (each such claim or demand, an, "Infringement Claim"). Also, notwithstanding the foregoing, Contractor shall defend, indemnify, and hold harmless the County Indemnitees from and against all Losses that could have been avoided by moving to a new release or version of the infringing software if such new release or version was reasonably available to Contractor and Contractor did not move to same. In the event of an Infringement Claim in which the County's right to use any technology or intellectual property is enjoined, Contractor shall either procure a license to enable the County to continue to use or receive the benefit of such technology or intellectual property or develop or obtain a non-infringing substitute acceptable to the County. Contractor shall have no obligation to indemnify, defend or hold the County Indemnitees harmless regarding any claim or action to the extent that it is based solely upon: (i) a modification of a program or machine by the County, any Third-Party contractor of the County that is not a Subcontractor, or any agent of the County that was not otherwise approved by Contractor; or (ii) the County's combination, operation, or use with apparatus, data, or programs neither furnished nor approved by Contractor nor contemplated by the Parties.

22.2. Injury, Property, or Other Damage

Without limiting Contractor's obligations with respect to insurance as provided in Section 19 hereof, Contractor shall indemnify, defend, and hold the County Indemnitees harmless with respect to any and all Losses related to any third-party claim alleging bodily injury or death, damage to tangible personal or real property, or any other damage, notwithstanding the form in which any such action is brought (e.g., contract, tort, or otherwise), to the extent such injuries or damages arise directly or indirectly from acts, errors, or omissions that constitute negligence, willful misconduct, or violations of law, by Contractor or its personnel, agents, or Subcontractors.

22.3. ThirdParty Contracts

Contractor shall indemnify, defend, and hold the County Indemnitees harmless from and against any and all Losses based upon or related to Third-Party services utilized by Contractor in providing Services or based upon an alleged breach by Contractor of any Third-Party agreement used by Contractor to provide the Services.

22.4. Misrepresentation

Contractor shall indemnify, defend, and hold the County Indemnitees harmless with respect to any and all Losses related to any third-party claim based upon or resulting from (i) any misrepresentation by Contractor in this Agreement, or (ii) theft, fraud, misappropriation of tangible or intangible personal property by Contractor or any Subcontractor, or by the officers, directors, Affiliates, employees, agents, representatives, or subcontractors of any of the foregoing.

22.5. Transitioned Employees

Contractor shall indemnify, defend, and hold the County Indemnitees harmless from and against any claim by any Transitioned Employee, and any and all Losses sustained or incurred by such County Indemnitees, based upon or resulting from any act by Contractor or its Subcontractors on or after the Cutover Date on which such Transitioned Employees transitioned to the employ of Contractor or a Subcontractor, or any allegation that such Transitioned Employee was wrongfully terminated by Contractor or was denied any severance or termination payment upon leaving the employ of Contractor. Contractor shall indemnify, defend, and hold harmless the County Indemnitees from and against any claim, and any and all Losses sustained or incurred by the County, by any of Contractor's employees (excluding Transitioned Employees) based upon or resulting from any act by Contractor.

22.6. Hazardous Material

Contractor shall indemnify, defend, and hold the County Indemnitees harmless from and against any claim by any third-party and any and all Losses sustained or incurred by such County Indemnitees as a result of: (i) Contractor's failure to comply in all material respects with any applicable Environmental Laws; (ii) the presence of any Hazardous Material upon, above, or beneath Contractor's facilities or locations, if the Hazardous Material was present or if the Hazardous Material was released into the environment by Contractor; or (iii) Contractor's breach of Section 20.10.

22.7. Proprietary Information Disclosure

Contractor shall indemnify, defend, and hold the County Indemnitees harmless from and against any and all Losses based upon or resulting from any third-party claim or challenge with respect to the disclosure or nondisclosure of Contractor Confidential Information or its Subcontractors' confidential or proprietary information under the California Public Records Act, or other applicable statutes or regulations, except to the extent that the County has failed to comply with its applicable policies with respect to the disclosure of such information.

22.8. General Obligation

Contractor's indemnity obligations under Sections 22.1, 22.2, 22.3, 22.4, 22.5, 22.6, and 22.7 of this Agreement also extend to third-party claims and associated Losses caused by the concurrent passive or vicarious negligence of any County Indemnitee. However, Contractor shall have no obligation to defend or indemnify the County Indemnitees to the extent third-party claims and associated Losses are caused by the active negligence, sole negligence, or willful misconduct of the County Indemnitees. If any legal action governed by this Section 22 is commenced against a County Indemnitee or a Contractor Indemnitee, such Party shall give written notice thereof to the indemnifying Party promptly after such legal action is commenced; provided, however, that failure to give prompt notice shall not reduce the indemnifying Party's obligations under this Section 22.8, except to the extent the indemnifying Party is prejudiced thereby. After such notice, if the indemnifying Party shall acknowledge in writing to the other Party that the right of indemnification under this Agreement applies with respect to such claim, then the indemnifying Party shall be entitled, if it so elects in a written notice delivered to the other Party not fewer than ten (10) days prior to the date on which a response to such claim is due, to take control of the defense and

investigation of such claim and to employ and engage attorneys of its choice, that are reasonably satisfactory to the other Party, to handle and defend same, at the indemnifying Party's expense. The other Party shall cooperate in all reasonable respects with the indemnifying Party and its attorneys in the investigation, trial, and defense of such claim and any appeal arising therefrom; provided, however, that the other Party may participate, at its own expense, through its attorneys or otherwise, in such investigation, trial, and defense of such claim and any appeal arising therefrom. No settlement of a claim that involves a remedy other than the payment of money by the indemnifying Party shall be entered into by the indemnifying Party without the prior written consent of the other Party, which consent may be withheld in the other Party's sole discretion. If the indemnifying Party does not assume the defense of a claim subject to such defense as provided in this Section, the indemnifying Party may participate in such defense, at its expense, and the other Party shall have the right to defend the claim in such manner as it may deem appropriate, at the expense of the indemnifying Party.

23. Dispute Resolution

23.1. Procedures To Be Established

If a dispute arises, the Parties' respective designated representatives shall meet and negotiate in good faith the resolution of such dispute. If such dispute cannot be promptly resolved, the County's representative and Contractor's Contract Manager shall meet and negotiate in good faith in order to resolve such dispute within ten (10) days after the date that written notice of dispute is delivered by the disputing Party to the other Party. If the County's representative and the Contract Manager have resolved the dispute, such Persons shall reduce the resolution to writing and each Party shall commence the resolution of the dispute in accordance therewith. In the event the County's representative and the Contract Manager have failed to resolve the dispute within ten (10) days after the referral of the dispute to them, the Parties shall refer the dispute to the County's CIO and the Contractor's Account Executive for resolution. If the CIO and the Contractor's Account Executive have resolved the dispute, such Persons shall reduce the resolution to writing and each Party shall commence the resolution of the dispute in accordance therewith. In the event the CIO and the Contractor's Account Executive have failed to resolve the dispute within thirty (30) days after the referral of the dispute to them, the Parties shall refer the dispute to the County's Assistant Chief Administrative Officer and the Contractor's Business Unit President. If the County's Assistant Chief Administrative Officer and the Contractor's Business Unit President are unable to resolve the Dispute, then the controversy may be resolved through any form of alternative dispute resolution as the Parties may agree or referred to a court of competent jurisdiction in the State of California. Notwithstanding the foregoing, either party shall be permitted to institute legal action under this Agreement on account of any such dispute without resorting to any or all of the dispute resolution procedure set forth herein.

23.2. De Minimis Disputes

Notwithstanding anything to the contrary provided in this Section 23 or elsewhere in this Agreement, if: (i) the County requests services, products, or resources from Contractor and the Parties disagree as to whether any such request is within the scope of the Services; and (ii) the financial impact on Contractor of satisfying such request, when aggregated with all other requests disputed and subject to this Section 23.2 in an applicable Contract Year, is less than two hundred

thousand dollars ($200,000.00), then the disagreement shall not be deemed a Problem, but absent mutual agreement of the Parties through the Management Committee, shall be deemed resolved in the County's favor; provided that the County provides to the Contractor a written notice expressly exercising its rights under this Section 23.2.

23.3. No Termination or Suspension of Services

Notwithstanding anything to the contrary contained herein, and even if any Problem or other dispute arises between the Parties and regardless of whether it requires at any time the use of any dispute resolution procedures established by the Parties in writing, in no event nor for any reason shall Contractor, during the Term of the Agreement or during Disentanglement, interrupt the provision of Services to the County, interrupt any obligations of or related to Disentanglement, disable any Hardware or Software used to provide Services, or perform any other action that prevents, impedes, or reduces in any way the provision of Services or the County's ability to conduct its activities, unless: (i) authority to do so is granted by the County Contracting Officer in writing or conferred by a court of competent jurisdiction; or (ii) the Term of this Agreement has been terminated or has expired pursuant to Section 17 hereof and a Disentanglement satisfactory to the County has been completed and County Contracting Officer has provided written notice thereof.

23.4. No Limitation on County Remedies for Default

The procedures established pursuant to this Section 23 shall not be deemed to limit the County's rights under Section 17 or either Party's rights under Section 18 in connection with a Default by either Party.

24. Other Miscellaneous

24.1. Entire Agreement

This Agreement, including the Schedules and Exhibits hereto, constitutes the entire understanding and agreement between the Parties with respect to the transactions contemplated herein and supersedes all prior or contemporaneous oral or written communications with respect to the subject matter hereof, all of which are merged herein. No usage of trade, or other regular practice or method of dealing between the Parties or others, may be used to modify, interpret, supplement, or alter in any manner the express terms of this Agreement.

24.2. Order of Precedence

In the event of conflict in substance or impact between the terms and conditions contained in Sections 1 through 24 of this Agreement and any terms and conditions contained in any Schedule, Attachment, or Exhibit hereto, the order of precedence in determining the controlling provision shall be as follows:

These terms and conditions and Schedule A, Defined Terms, together; then

Appendices to Schedule A, Defined Terms; then

Schedule 19, Insurance Requirements; then

Schedule 4.3, Operational Services; then

Schedule 16.1 Fees; then

Exhibit 16.1-1 through Exhibit 16.1-7, in order of exhibits; then

Schedule 4.8, Service Levels; then

Exhibit 4.8-1, Special Service Level Requirement; then

Schedule 2.1, Transition Plan; then

Schedule 16.8, Fee Reductions; then

Schedule 16.7, Benchmarking Methodology; then

Schedule 18.2, Third Party Contracts; then

Schedule 12.1.1, Information Privacy and Security, Criminal Offender Record Information, California Law Enforcement Telecommunication Systems, and County Facility Access; then

Exhibit 12.1.1-1 through Exhibit 12.1.1-5, in order of exhibits; then

Schedule 14.1, Approved Subcontractors; then

Schedule 10.1.1, Contractor Key Personnel; then

Schedule 10.3, Relationship Management; then

Except as set forth below, schedules and then exhibits in sequential order; then

Appendix 4.3.1, Contractor's Solution; then

Schedule 1.2, Offeror's Proposal.

24.3. Conflicts, Errors, Omissions, and Discrepancies

In case of conflicts, discrepancies, errors, or omissions among the various parts of this Agreement, any such matter shall be submitted immediately by Contractor to the County for clarification. The County shall issue such clarification within a reasonable period of time. Any Services affected by such conflicts, discrepancies, errors or omissions that are performed by Contractor prior to clarification by the County shall be at Contractor's risk.

24.4. Updates

The information contained in the Schedules, Attachments, Exhibits, and Appendixes hereto will be updated in a timely manner by the Contractor, at no additional cost, from time to time during the Term to accurately reflect the evolution of the Services and components and elements of the Services as described therein, and such updates will be delivered to the County for the County's approval, and, upon the County's approval, will be incorporated into the Agreement.

24.5. Captions; References; Terminology

Captions, Tables of Contents, Indices of Definitions, and Schedule and Exhibit titles are used herein for convenience of reference only and may not be used in the construction or interpretation of this

Agreement. Any reference herein to a particular Section number (e.g., "Section 2"), shall be deemed a reference to all Sections of this Agreement that bear sub-numbers to the number of the referenced Section (e.g., Sections 2.1, 2.1.1, etc.). Any reference herein to a particular Schedule or Exhibit (e.g., Schedule 4.3) shall be deemed a reference to the Schedule hereto that bears the same number. As used herein, the word "including" shall mean "including, but not limited to." The Parties agree that the use of the phrase "at no additional cost" or similar throughout this Agreement is to provide additional clarity and is not intended to create any inference that Contractor may impose additional charges (other than those set forth in Schedule 16.1) with respect to any Contractor obligations hereunder the description of which is not accompanied by such phrase or similar phrase. Any reference in this Agreement to "days" shall mean calendar days unless expressly identified as "business days."

24.6. Assignment

Except for subcontracting permitted under the terms of Section 14 hereof, neither this Agreement, nor any interest therein, nor any of the rights and obligations of Contractor hereunder, may be directly or indirectly assigned, sold, delegated, or otherwise disposed of by Contractor, in whole or in part, without the prior written consent of the County, which may be withheld in its sole discretion. County may, at its sole discretion, authorize the assignment of all or a part of Contractor's rights or obligations or both, under this Agreement.

24.7. Notices to a Party

Except as expressly otherwise stated herein, all notices, requests, consents, approvals, or other communications provided for, or given under, this Agreement, shall be in writing and shall be deemed to have been duly given to a Party if delivered personally, or transmitted by facsimile or electronic mail to such Party at its telecopier number or e-mail address set forth below (with the original sent by recognized overnight courier or first-class mail to the Party at its address set forth below), or sent by first class mail or overnight courier to such Party at its address set forth below, or at such other telecopier number or address, as the case may be, as shall have been communicated in writing by such Party to the other Party in accordance with this Section. All notices shall be deemed given when received in the case of personal delivery or delivery by mail or overnight courier, or when sent in the case of transmission by facsimile or electronic mail with a confirmation, if confirmed by copy sent by overnight courier within one (1) day of sending the facsimile.

Notices to the County shall be addressed as follows:

County of San Diego
Chief Information Officer
1600 Pacific Highway

Room 306F
San Diego, California 92101

Facsimile No.: (619) 685-2427

with a copy to the attention of the County's counsel addressed as follows:

County of San Diego
County Counsel
1600 Pacific Highway
Room 355
San Diego, California 92101
Facsimile No.: (619) 531-5506

Notices to Contractor shall be addressed as follows:

Account Executive
15231 Avenue of Science
San Diego, CA 92128
Attention: Julie Waddell, Sr. Director
Email: Julie.waddell@peraton.com

with a copy to the attention of Contractor's general counsel at:

Office of the General Counsel

1875 Explorer St
Reston, VA 20190
Attention: Jim Winner
Email: jwinner@peraton.com

24.8. Amendments; Waivers

Except as expressly provided herein, this Agreement may not be modified, amended, or in any way altered except by a written document duly executed by both of the Parties hereto. The County's Contracting Officer is the only County employee authorized to modify or amend this Agreement; the CIO has no authority to modify or amend this Agreement. No waiver of any provision of this Agreement, nor of any rights or obligations of any Party hereunder, shall be effective unless in writing and signed by the Party waiving compliance, and such waiver shall be effective only in the specific instance, and for the specific purpose, stated in such writing. No waiver of breach of, or

default under, any provision of this Agreement shall be deemed a waiver of any other provision, or of any subsequent breach or default of the same provision, of this Agreement.

24.9. Relationship Between, and Legal Status of, the Parties

This Agreement shall not be construed to deem either Party as a representative, agent, employee, partner, or joint venturer of the other. Contractor shall be an independent contractor for the performance under this Agreement. Contractor shall not have the authority to enter into any agreement, nor to assume any liability, on behalf of the County, nor to bind or commit the County in any manner, except as provided hereunder. Contractor's employees who provide services pursuant to this Agreement or who are located on the County's premises shall remain employees of Contractor, and Contractor shall have sole responsibility for such employees including responsibility for payment of compensation to such personnel and for injury to them in the course of their employment. Contractor shall be responsible for all aspects of labor relations with such employees including their hiring, supervision, evaluation, discipline, firing, wages, benefits, overtime and job and shift assignments, and all other terms and conditions of their employment, and the County shall have no responsibility therefor. Contractor shall defend, indemnify, and hold harmless County Indemnitees from and against any and all Losses based upon or related to a claim that Contractor's or its Subcontractors' employees are employees of the County.

24.10. Severability

If any provision of this Agreement is determined to be invalid or unenforceable, that provision shall be deemed stricken and the remainder of this Agreement shall continue in full force and effect insofar as it remains a workable instrument to accomplish the intent and purposes of the Parties; the Parties shall replace the severed provision with the provision that will come closest to reflecting the intention of the Parties underlying the severed provision but that will be valid, legal, and enforceable.

24.11. Counterparts

This Agreement may be executed in duplicate counterparts. Each such counterpart, if executed by both Parties, shall be an original and both together shall constitute but one and the same document. This Agreement shall not be deemed executed unless and until at least one counterpart bears the signatures of both Parties' designated signatories.

24.12. Laws and Regulations

This Agreement shall be interpreted under, and governed by, the laws and court decisions of the State of California and the United States of America, without giving effect to the State's principles of conflicts of laws.

24.13. County Approval of Promotions

Unless specifically authorized in writing by the CIO and the County on a case-by-case basis, Contractor shall have no right to use, and shall not use, the name of the County, its departments, officials, or employees, or the seal of the County: (i) in any advertising, publicity, promotion; or (ii) to express or to imply any endorsement of Contractor's products or services; or (iii) in any other manner (whether or not similar to uses prohibited by subparagraphs (i) and (ii) above), except only to deliver the Services in accordance with this Agreement.

24.14. Venue and Jurisdiction

All actions or proceedings arising out of, or related to, this Agreement shall be brought only in an appropriate federal or State court in San Diego, California and the Parties hereby consent to the jurisdiction of such courts over themselves and the subject matter of such actions or proceedings. Contractor hereby appoints Contractor's General Counsel and his or her successors in office to be its agent upon whom any process, in any action or proceeding against it arising out of this Agreement, may be served.

24.15. Governmental Immunity

Notwithstanding any provisions to the contrary contained in this Agreement, it is agreed and understood that the County shall not be construed to have waived any rights or defenses of governmental immunity that it may have with respect to all matters arising out of this Agreement.

24.16. No ThirdParty Beneficiaries

This Agreement is an agreement between the Parties, and, except as provided in this Section 24.16, this Agreement confers no rights upon any of the Parties' employees, agents, or contractors, or upon any other Person; provided, however, that the Superior Court of California, County of San Diego shall be deemed a third-party beneficiary of this Agreement and shall have the rights, and Contractor shall have the obligations, with respect to the Superior Court of California, County of San Diego, as set forth in this Agreement.

24.17. Expenses

Each Party shall pay all expenses paid or incurred by it in connection with the planning, negotiation, and consummation of this Agreement, subject to the provisions of Section 18.2.

24.18. Survival

The provisions of Sections 6, 12, 13, 14, 15, 18, 19, 20, 21, 22, 23, 24, and any Sections of this Agreement that by their nature may reasonably be presumed to survive any termination or expiration of this Agreement, shall survive any termination or expiration hereof.

24.19. Neither Party Considered Drafter

Despite the possibility that one Party may have prepared the initial draft of this Agreement or played the greater role in the physical preparation of subsequent drafts, the Parties agree that neither of them shall be deemed the drafter of this Agreement and that, in construing this Agreement in case of any claim that any provision hereof may be ambiguous, no such provision shall be construed in favor of one Party on the ground that such provision was drafted by the other.

24.20. NonSolicitation

Neither Contractor nor any of its Subcontractors shall directly solicit any County employee for any employment opportunities with Contractor or any Subcontractor. The County recognizes that its employees may respond to Contractor's (or its Subcontractors') generally available advertisements, job postings, or web sites, without solicitation by Contractor or any Subcontractor. In the event that a County employee approaches Contractor (or any of its Subcontractors) in connection with an employment opportunity, Contractor (or the applicable Subcontractor) shall (i) take no action with respect to such employee other than to refer such employee to Contractor's or Subcontractor's

human resources department so that the employment interest may be officially logged, and (ii) inform the County's CIO of the specific employee expressing interest in employment with Contractor or the applicable Subcontractor. Within five (5) business days, the County's CIO will inform Contractor's Contract Manager whether Contractor (or its Subcontractor) may hire the applicable County employee, and whether such employee would be allowed to provide Services to the County if hired by Contractor (or its Subcontractor). Contractor hereby agrees that neither it nor any of its Subcontractors shall hire any County employee without receiving the prior written consent of the County.

24.21. Reserved

****

(Signature Page Follows)

The Parties have executed this Information Technology and Telecommunications Services Agreement on the dates of the signatures of their respective representatives below.

COUNTY OF SAN DIEGO

ALLEN HUNSBERGER, Acting Director

Department of Purchasing and Contracting

By: Allen Hunsberger (Jan 10, 2025 11:42 PST)

Name: Allen Hunsberger

Title: Assistant Director, Purchasing and Contr

Date: Jan 10, 2025

PERATON ENTERPRISE SOLUTIONS LLC

By:

Name: Max Pinna

Title: Contracts Manager

Email: max.pinna@peraton.com

Date: Jan 6, 2025

By electronically signing this document, all parties accept the use of electronic signatures.

Adobe Acrobat Sign Transaction Number: CBJCHBCAABAARUJkUa_prWg9NU23snQRcPYmqn9CRwwW

Approved as to form and legality.

County Counsel

By: Inna Zazulevskaya

Name: Inna Zazulevskaya Title: Senior Deputy County Counsel Date: Jan 9, 2025

Schedule A – Definitions

Table of Contents

1. Acceptance....10
2. Acceptance Criteria....10
3. Acceptance Review Procedures....10
4. Acceptance Review Period....10
5. Accepted Schedule and Budget....10
6. Access Line....10
7. ADA....10
8. Add....11
9. Affiliate....11
10. Agreement....11
11. Application....11
12. Application Development Server....11
13. Application Pre-Production Server....11
14. Application Priority....12
15. Application Production Server....12
16. Application Rate....12
17. Application Server....12
18. Application services....12
19. Applications Suite....13
20. Application Test Server....13
21. Asset....13
22. Assigned Contracts....13
23. Assigned Leases....14
24. At-Risk Amount....14
25. At-Risk Pool....14
26. Availability....14
27. Availability of Application....14
28. Availability of Support Staff....15
29. Banding....15

30. Baseline Volume....15
31. Bundled Resource Units....15
32. Business Groups....15
33. California Public Records Act....15
34. Change in Control....15
35. CIO....15
36. Client Satisfaction....16
37. Computing Service Registration Form (CSRF)....16
38. Conditional Acceptance....16
39. Confidential Information....16
40. Contingent Work....16
41. Contingent Work Request....16
42. Contract Manager....16
43. Contract Year or CY....17
44. Contracting Officer....17
45. Contractor....17
46. Contractor Confidential Information....17
47. Contractor Indemnitees....17
48. Contractor Key Personnel....18
49. Contractor Named Personnel....18
50. Contractor Software....18
51. Contractor Works....18
52. Control....18
53. COTS....18
54. County....19
55. County Confidential Information....19
56. County Data....20
57. County Facilities....21
58. County Holidays....21
59. County Indemnitees....21

60. County Software 21
61. County Works 21
62. Critical Milestones 22
63. Cross Functional Services 22
64. Current Projects 22
65. Current Services 22
66. Cutover 23
67. Cutover Date 23
68. Data Center 23
69. Data center services 23
70. Data Network 23
71. Decommission 24
72. Default 24
73. Deficiency(ies) 26
74. Demand Batch Jobs 26
75. Designated Employees 27
76. Desktop Application 27
77. Desktop Computing Services 27
78. Development 27
79. Disabling Device 27
80. Disentanglement 27
81. Disentanglement Services 27
82. Effective Date 27
83. End-to-End Response Time 28
84. End-User or User 28
85. End-User Services 28
86. Environmental Laws 28
87. Exception Report 29
88. Expiration Date 29
89. Failure 29

90. Fee Reduction 29
91. Fees 29
92. Final Acceptance 29
93. Final Acceptance Criteria 29
94. Final Acceptance Review Period 29
95. Final Acceptance Review Procedures 30
96. Force Majeure Event 30
97. Framework Component 30
98. GAAP 30
99. Government Approvals 30
100. Hazardous Materials 31
101. Hardware 31
102. High Response End-User 31
103. Immediately 31
104. Incident 31
105. Including 32
106. Infrastructure server 32
107. Infringement Claim 32
108. Initial Term 32
109. Install 32
110. Intellectual Property Rights 32
111. IT 33
112. Key Subcontractors 33
113. Known Defect 33
114. Large Work Request 33
115. Latent Defect 33
116. Legacy Provider 34
117. Level of Effort (LOE) Work Request 34
118. Local Area Network or LAN 34
119. Location 34

120. Losses 34
121. Machines 35
122. Management Committee 35
123. Maximum Annual Fee 35
124. Measurement Period 35
125. Medium Work Request 36
126. Middleware 36
127. Milestone 36
128. Minimum Performance 36
129. Mission / Business Critical 36
130. Month 36
131. Monthly Services Charge (MSC) 37
132. Move 37
133. Net Book Value (NBV) 37
134. Network Services 37
135. No Defect 37
136. Online Transaction Response Time 37
137. Optional Item Catalog or OIC 38
138. Party 38
139. Performance Target 38
140. Person 38
141. Point of Presence (Pop) 38
142. Planned Outages 38
143. Portfolio Application List 39
144. Portfolio Applications 39
145. Premises Devices 39
146. Problem 39
147. Problem Resolution Report 39
148. Project 40
149. Project Estimation 40

150. Provisional Termination Date 40
151. Public Record Data 40
152. Public Switched Telephone Network (PSTN) 40
153. Purchased Assets 40
154. Quality 41
155. Remote Access Request Form (RARF) 41
156. Remove 41
157. Reporting Interval 41
158. Reporting Period 41
159. Request for Network Access (RFNA) Form 42
160. Required Consents 42
161. Residuals 42
162. Resolve 42
163. Respond Time (Time to Respond) 43
164. Resource Unit (RU) 43
165. Resource Unit Fee 43
166. Resolved 43
167. Response Time of the Application 43
168. Retained Assets 44
169. Retained Desktop Computers 44
170. Retirement 44
171. Root-Cause Analysis 44
172. Sales Tax(es) 44
173. Scheduled Maintenance 44
174. Scheduled Time 45
175. Scheduled Uptime 45
176. SEI/CMM Level 45
177. Servers 45
178. Service Desk Services 45
179. Service Framework 46

180. Service Level (SL) 46
181. Service Portal 46
182. Service Request 46
183. Services 46
184. Shared Resources 47
185. Site 47
186. Software 47
187. Specifications 48
188. Standards and Procedures Manual (SnP Manual) 48
189. State 48
190. Subcontractor 48
191. System 48
192. System of Record 48
193. Target 49
194. Task-Based Service Request 49
195. Term 49
196. Terminated Services 49
197. Termination Date 49
198. Termination Notice 49
199. Third-Party 49
200. Third-Party Resources 50
201. Third-Party Software 50
202. Third-Party Works 50
203. Ticket 50
204. Transition 50
205. Transition Plan 50
206. Transitioned Employee 51
207. Underlying Works 51
208. UNIX Server 51
209. Unscheduled Maintenance 51

210. Voice Services 52
211. Voice Switch or PBX 52
212. WARN Act 52
213. WARN Notice 53
214. Week 53
215. Weighting Factor 53
216. WIDE AREA NETWORK or WAN 53
217. Work Product 53
218. Workstation 54

The following words and phrases, when used in the Agreement, shall have the indicated meanings. (Terms capitalized within a particular definition have been defined elsewhere within the Agreement.)

1. ACCEPTANCE

"Acceptance" shall have the meaning given to it in Section 9.10.1 of the Agreement.

2. ACCEPTANCE CRITERIA

"Acceptance Criteria" shall have the meaning given to it in Section 9.10.1 of the Agreement.

3. ACCEPTANCE REVIEW PROCEDURES

"Acceptance Review Procedures" shall have the meaning given to it in Section 9.10.1 of the Agreement.

4. ACCEPTANCE REVIEW PERIOD

"Acceptance Review Period" shall have the meaning given to it in Section 9.10.1 of the Agreement.

5. ACCEPTED SCHEDULE AND BUDGET

"Accepted Schedule and Budget" shall mean a Project plan and budget that has been mutually agreed to by the County and Contractor.

6. ACCESS LINE

"Access Line" shall mean the connection between a customer premises network interface and the Local Exchange Carrier (LEC) that provides access to the PSTN.

7. ADA

"ADA" shall have the meaning given to it in Section 20.3 of the Agreement.

8. ADD

"Add" shall mean providing additional functionality to an existing Asset.

9. AFFILIATE

"Affiliate" shall mean, as to any Person, any other Person that, directly or indirectly, controls, is controlled by, or is under common control with, such Person, whether through ownership of voting securities or otherwise. For this purpose, and without limiting the foregoing, any Person that owns more than twenty percent (20%) of the outstanding voting securities of any other Person shall be deemed to control such other Person.

10. AGREEMENT

"Agreement" shall mean this Information Technology and Telecommunications Services Agreement including all attachments, Schedules, Exhibits, Appendices, and hereto, as amended or restated from time-to-time.

11. APPLICATION

"Application" means Software to provide specific functionality in support of one or more business processes.

12. APPLICATION DEVELOPMENT SERVER

"Application Development Server" shall mean any Server used in the design and build of an Application

13. APPLICATION PRE-PRODUCTION SERVER

"Application Pre-Production Server" shall mean any Application Server that is built and made ready for deployment prior to the County's Acceptance of the Application as the System of Record.

14. APPLICATION PRIORITY

Applications shall be classified info the following Priorities:

- Priority 1 (P1) – Life/Health/Safety-related Applications
- Priority 2 (P2) – Mission/Business Critical Applications
- Priority 3 (P3) – All other Applications

15. APPLICATION PRODUCTION SERVER

"Application Production Server" means a Server that hosts an Application that is considered to be the System of Record.

16. APPLICATION RATE

"Application Rate" shall mean any one of the hourly rates included within the schedule of Application Services Labor rates for various categories of Contractor personnel as set forth in Exhibit 16.1-4 to Schedule 16.1.

17. APPLICATION SERVER

"Application Server" shall mean any Server that hosts Portfolio Applications that are identified in the Portfolio Application List (or intended to be added) as listed in the Standards and Procedures Manual. Application Servers also host such services as business rule execution, browser based presentation and database management systems.

18. APPLICATION SERVICES

"Application Services" shall mean the Services described in Section 7 of Schedule 4.3-Operational Services.

19. APPLICATIONS SUITE

"Applications Suite" means a combination of Applications sold or developed as an integrated product (e.g., Oracle Financials, IPTS).

20. APPLICATION TEST SERVER

"Application Test Server" shall mean a dedicated Server used in the test phase of Application development, as designated by the County.

21. ASSET

"Assets" shall mean Hardware and Software and all other intangible and tangible items, including personal and real property, and employees, agents, Subcontractors and vendors, used to provide the Services.

22. ASSIGNED CONTRACTS

"Assigned Contracts" shall mean those written maintenance agreements, service contracts, Software license agreements, and Subcontractor agreements under which the County receives Third-Party services (either directly or through the Legacy Provider, or any Subcontractor or Third-Party of the Legacy Provider) relating to its IT and Telecommunications requirements listed on Appendix A.2 and such others relating to the Services as may be identified by the County in a written notice delivered to Contractor, that the County or the Legacy Provider (or any Subcontractor of the Legacy Provider) will assign to Contractor pursuant to an Assignment and Assumption Agreement. After the Signing Date, if Contractor identifies a maintenance agreement, service contract, Software license agreement, or Subcontractor agreement relating to the Services that was inadvertently omitted from Appendix A.2, Contractor shall notify the County in writing and the Parties shall make a reasonable accommodation therefor.

23. ASSIGNED LEASES

"Assigned Leases" shall mean those equipment leases listed on Appendix A.3, and such other leases relating to the Services as may be identified by the County in a written notice delivered to Contractor after the Signing Date, that the County or the Legacy Provider (or any Subcontractor of the Legacy Provider) will assign to Contractor pursuant to an Assignment and Assumption Agreement. After the Signing Date, if Contractor identifies an equipment lease relating to the Services that was inadvertently omitted from Appendix A.3, Contractor shall notify the County in writing and the Parties shall make a reasonable accommodation therefor.

24. AT-RISK AMOUNT

"At-Risk Amount" shall have the meaning set forth in Schedule 16.8.

25. AT-RISK POOL

"At-Risk Pool" shall have the meaning set forth in Schedule 16.8.

26. AVAILABILITY

"Availability" shall mean the percentage of time a given service is fully operational. Availability represents a measure of the fraction of time during a defined period when the service provided is deemed to be better than the defined Service Level.

Availability (%) = 100% – Unavailability (%)

Where Unavailability is defined as:

$$\frac{\sum \text{Outage Duration} \times 100\%}{\text{Schedule Time} - \text{Planned Outages}}$$

27. AVAILABILITY OF APPLICATION

"Availability of Application" shall mean the time an Application will be running and operable according to the Service Levels.

28. AVAILABILITY OF SUPPORT STAFF

"Availability of Support Staff" shall mean the schedule of time that the Contractor will have staff available to respond to Service Requests or Incidents.

29. BANDING

"Banding" shall have the meaning set forth in Schedule 16.1.

30. BASELINE VOLUME

"Baseline Volume" shall have the meaning set forth in Schedule 16.1.

31. BUNDLED RESOURCE UNITS

"Bundled Resource Units" shall have the meaning set forth in Schedule 16.1.

32. BUSINESS GROUPS

"Business Groups**"** shall mean the County's operational groups known as the Finance and General Government Group ("FG3"), Health and Human Services Agency ("HHSA"), Land Use and Environmental Group ("LUEG"), and Public Safety Group ("PSG").

33. CALIFORNIA PUBLIC RECORDS ACT

"California Public Records Act" shall have the meaning given to it in Section 12.3.3 of the Agreement.

34. CHANGE IN CONTROL

"Change in Control" shall have the meaning given to it in Section 17.2.2 of the Agreement.

35. CIO

The term "CIO" the acronym for "Chief Information Officer," shall mean the County's executive officer responsible for oversight of the Services.

36. CLIENT SATISFACTION

"Client Satisfaction" shall mean a subjective rating obtained through a combination of periodic client surveys and feedback from random caller follow up calls.

37. COMPUTING SERVICE REGISTRATION FORM (CSRF)

"Computing Service Registration Form" or "CSRF" shall mean the Service Request form used to request access to various levels of computing resources.

38. CONDITIONAL ACCEPTANCE

"Conditional Acceptance" shall have the meaning given to it in Section 9.10.1 of the Agreement.

39. CONFIDENTIAL INFORMATION

"Confidential Information" shall mean the County Confidential Information or the Contractor Confidential Information, as the case may be.

40. CONTINGENT WORK

"Contingent Work" shall mean defect work that is pre-authorized for Incident ticket resolution only.

41. CONTINGENT WORK REQUEST

"Contingent Work Request" shall mean a Service Request that is pre-authorized for Incident ticket resolution only.

42. CONTRACT MANAGER

"Contract Manager" shall mean, initially, the Contractor employee who is so designated in Schedule 10.1.1 and, thereafter, any subsequent holder of that position designated and approved in accordance with Section 10.1.1 of the Agreement.

43. CONTRACT YEAR OR CY

"Contract Year" or "CY" shall mean:

(i) the period beginning on the Effective Date and ending on December 31, 2017;

(ii) each of the next succeeding twelve-month (12) periods beginning on January 1st and ending on December 31st;

(iii) if applicable, each period in respect to which the County elects to extend the effective date of any expiration or termination of the Term from the beginning of the extension period until its last day, for each extension period.

44. CONTRACTING OFFICER

"Contracting Officer" shall mean the County's Director of Purchasing and Contracting, or his or her designee, who shall have the responsibilities described in the Agreement.

45. CONTRACTOR

"Contractor" shall have the meaning given to it in the introduction to the Agreement.

46. CONTRACTOR CONFIDENTIAL INFORMATION

"Contractor Confidential Information" shall have the meaning given to it in Section 12.10 of the Agreement (Contractor Confidential Information).

47. CONTRACTOR INDEMNITEES

"Contractor Indemnitees" shall mean Contractor, and each of its officers, directors, employees, agents, successors, and assigns.

48. CONTRACTOR KEY PERSONNEL

"Contractor Key Personnel" shall mean, initially, those personnel of Contractor and its Subcontractors who are so designated in Schedule 10.1.1 and, thereafter, their respective replacements as designated and approved in accordance with Section 10 of the Agreement.

49. CONTRACTOR NAMED PERSONNEL

"Contractor Named Personnel" shall mean those personnel of Contractor and its Subcontractors who are so designated in Report 42 – Contractor Organizational Chart.

50. CONTRACTOR SOFTWARE

"Contractor Software" means Contractor Works comprising Software and all supporting documentation, media, and related materials, provided or made available to the County or otherwise used by Contractor or its Subcontractors in connection with the performance of the Services, including the Software that is specifically identified in Appendix A.4 hereto (including all updates, enhancements, customizations, and other improvements thereof).

51. CONTRACTOR WORKS

"Contractor Works" means Underlying Works conceived, invented, created, or acquired by Contractor or a Subcontractor, rather than by a Third-Party.

52. CONTROL

"Control" shall have the meaning given to it in Section 17.2.2 of the Agreement.

53. COTS

"COTS" or "Commercial Off-The-Shelf" means any Software that is developed at the expense of a Third-Party and is normally commercially available for acquisition and use by multiple customers.

54. COUNTY

"County" shall have the meaning set forth in the introduction to the Agreement. For purposes of the performance of Contractor's obligations under the Agreement, the term "County" shall be deemed to include the Superior Court of California, County of San Diego so long as, and to the extent that the Superior Court receives Services under the Agreement.

55. COUNTY CONFIDENTIAL INFORMATION

"County Confidential Information" shall mean records, data, and other information that is obtained by Contractor or any of its employees, or Subcontractors from (or with regard to) the County in connection with the performance of the Agreement, whether in tangible or intangible form, and whether in written form or readable by machine, and including:

(i) all County Data;

(ii) all Public Record Data (except as provided below);

(iii) all financial information, personnel information, reports, documents, correspondence, plans, and specifications relating to the County;

(iv) all technical information, materials, data, reports, programs, documentation, diagrams, ideas, concepts, techniques, processes, inventions, knowledge, know-how, and trade secrets, developed or acquired by the County, including Work Product;

(v) any information that the County identifies to Contractor as confidential by a stamp or other similar notice; and

(vi) all other records, data, or information collected, received, stored, or transmitted in any manner connected with the provision of Services hereunder.

County Confidential Information shall not include information that Contractor can demonstrate was:

(i) at the time of disclosure to Contractor, in the public domain;

(ii) after disclosure to Contractor, published or otherwise made a part of the public domain through no fault of Contractor;

(iii) in the possession of Contractor at the time of disclosure to it, if Contractor was not then under an obligation of confidentiality with respect thereto;

(iv) received after disclosure by the County to Contractor from a Third-Party who had a lawful right to disclose such information to Contractor; or

(v) independently developed by Contractor without reference to County Confidential Information. Additionally, County Confidential Information shall not include Public Record Data to the extent disclosure of such data is required by the California Public Records Act, as determined by the County in its sole discretion. For purposes of this provision, information is in the public domain if it is generally known (through no fault of Contractor) to Third-Parties who are not subject to nondisclosure restrictions similar to those in the Agreement.

56. COUNTY DATA

"County Data" shall mean, in or on any media or form of any kind: (i) all data and summarized data related to the County, its citizens, or the Services and all data concerning or indexing such data (regardless of whether or not owned by the County, generated or compiled by the County, or provided by its citizens), including data that is in the County's databases or otherwise in the County's possession on the Effective Date or at any time during the Term; (ii) all other County records, data, files, input materials, reports, forms, and other such items that may be received, computed, developed, used, or stored by Contractor, or by any of its Subcontractors, in the performance of Contractor's duties under the Agreement; and (iii) with regard to any of the information in (i) or (ii), any modification, compilation, or derivative work thereof.

57. COUNTY FACILITIES

"County Facilities" shall have the meaning given to it in Section 8.1 of the Agreement.

58. COUNTY HOLIDAYS

"County Holidays" shall mean those holidays established per Article III, Section 57 of the County Administrative Code; and for the Superior Court, those holidays established per California Government Code Sections 19851-19855.

59. COUNTY INDEMNITEES

"County Indemnitees" shall mean the County, all of its agencies, departments and subdivisions, and each of their respective officers, directors, elected officials, employees, agents, successors, and assigns.

60. COUNTY SOFTWARE

"County Software" means all Software that is conceived, invented, created, developed, or otherwise acquired by the County before, on, or after the Effective Date, and all supporting documentation, media, and related materials, and all modifications, enhancements, updates, replacements, and other derivative works of any of the foregoing, but excluding the Contractor Software and the Third-Party Software.

61. COUNTY WORKS

"County Works" means all tangible and intangible information and developments that:

(i) were conceived, invented, created, developed or acquired by the County prior to the Effective Date; or

(ii) are conceived, invented, created, developed or otherwise acquired by the County on or after the Effective Date, but only to the extent such information and developments do not constitute Work Product hereunder. County Works include

all intermediate and partial versions thereof, including all source code and object code with respect thereto, and all processes, methods, apparati, programs, procedures, designs, Specifications, inventions, discoveries, improvements, ideas, know how, techniques, materials, program materials, County Software (to the fullest extent of the County's rights therein), flow charts, notes, outlines, lists, compilations, manuscripts, writings, reports, data, data models, pictorial materials, schematics, other creations, and the like, whether or not patented or patentable or otherwise protectable by law.

62. CRITICAL MILESTONES

"Critical Milestones" shall mean those actions and projects identified during the Term in accordance with Section 4.12 of the Agreement.

63. CROSS FUNCTIONAL SERVICES

"Cross Functional Services" shall mean the services described in Section 2 of Schedule 4.3 – Operational Services. Cross Functional Services shall apply to all the Services Frameworks.

64. CURRENT PROJECTS

"Current Projects" shall mean all IT and telecommunications-related development efforts, as specified by the County, that were in progress as of the Cutover Date.

65. CURRENT SERVICES

"Current Services" shall mean the IT and telecommunications services and functions being performed for the County at any time during the twelve (12) calendar months preceding the month in which the Cutover Date occurs, including those being performed by: (i) the Legacy Provider, (ii) Designated Employees; (iii) other County employees that provided IT and Telecommunications Services and functions similar to those provided by the Designated Employees but whose positions are vacant on the Cutover Date; and (iv) any other Persons

providing IT and Telecommunications Services or functions to the County, including provision by means of any contract.

66. CUTOVER

"Cutover" shall mean, with respect to each Service Framework, the successful completion of the Services related to the Transition of such Service Framework from the Legacy Provider to Contractor (including the completion of all milestones set forth in the Transition Plan pertaining to such Service Framework), as approved by the County and confirmed by the Legacy Provider in writing.

67. CUTOVER DATE

"Cutover Date" shall mean the date specified in the Transition Plan corresponding to when Cutover for a particular Service Framework shall occur and the Contractor will have full operational responsibility for the performance of the Services under such Service Framework. There will be one Cutover Date corresponding to each Service Framework.

68. DATA CENTER

"Data Center" shall mean locations, one or more, containing Data Center Assets, as defined in Section 6 of Schedule 4.3 – Operational Services.

69. DATA CENTER SERVICES

"Data Center Services" shall mean the Services described in Section 6 of Schedule 4.3 – Operational Services.

70. DATA NETWORK

"Data Network" shall mean the network that is comprised of the Services and Assets defined in Section 5 of Schedule 4.3 – Operational Services.

71. DECOMMISSION

"Decommission" shall mean the work required to take an Application out of service.

72. DEFAULT

"Default" shall mean the occurrence of any of the following:

(i) With respect to Contractor, the occurrence of any of the following:

a) Contractor's failure to provide the Services in accordance with the Service Levels if Contractor fails to use its best efforts (that shall not involve the payment of funds that would not be commercially reasonable under the circumstances) to correct such failure or if, notwithstanding such best efforts, Contractor fails to meet a single Service Level in three (3) or more of any six (6) consecutive Measuring Periods for such Service Level. (For purposes of this paragraph (i)(a), the words "correct" and "corrected" shall include implementation of a work-around or similar temporary measure, provided that Contractor continues utilization of its best efforts (that shall not involve the payment of funds that would not be commercially reasonable under the circumstances) to pursue and promptly implement a full and complete cure);

b) Contractor fails to provide the Services in accordance with the Service Levels or fails to meet Critical Milestones such that Contractor is assessed total Fee Reductions in any calendar month in excess of ten percent (10%) of that month's At Risk Amount or Contractor fails to provide the Services in accordance with the Service Levels or fails to meet Critical Milestones such that at any time during the Contract Year, the Contractor's cumulative Fee Reductions are in excess of five percent (5%) of that Contract Year's At Risk Amount;

c) a failure by Contractor to use all commercially reasonable efforts to avert, prevent, avoid, or remedy any interruption or shutdown (of any material duration) of any essential County facility or operation, including communications networks

utilized by any part of the County providing public safety, health, corrections, military, emergency, or financial disbursement services;

d) a breach by Contractor of any obligation under Section 12 or Section 15 of the Agreement, provided that such breach, if curable, is not cured within thirty (30) days after Contractor has received notice of such breach;

e) the discovery that a representation made in the Agreement by Contractor was false when made, if the nature and magnitude of the misrepresentation are such as to have had a probable and material effect upon the County's decision to engage Contractor or upon the negotiations as to the other terms of the Agreement;

f) a judicial declaration of the insolvency of Contractor; the general failure of Contractor to pay its debts in the normal course of business; the entrance of Contractor into receivership or any arrangement or composition with creditors generally; the filing of a voluntary or involuntary petition that is not dismissed within sixty (60) days for the bankruptcy, reorganization, dissolution, or winding-up of Contractor; a general assignment for the benefit of creditors of Contractor; or a seizure or a sale of a material part of Contractor's property by or for the benefit of any creditor or governmental agency;

g) an assignment or attempted assignment by Contractor in violation of Section 24.6 of the Agreement;

h) debarment of Contractor from performing services with respect to all business with the federal government; or

i) a material breach by Contractor of any of its other obligations under the Agreement and (A) the failure by Contractor to cure such breach within thirty (30) days after Contractor has received written notice of such breach; or (B) if the failure is not one that could reasonably be corrected within thirty (30) days, (1) the failure by Contractor to adopt, within thirty (30) days after receiving notice of such breach,

a plan to cure such breach within a time period not longer than sixty (60) days after Contractor received notice of the breach, or (2) the failure by Contractor to cure such breach within such sixty (60)-day period.

(ii) With respect to the County, the occurrence of any of the following:

a) breach by the County in making payment of any amount payable to Contractor under the Agreement (subject to the provisions of Section 16.12 of the Agreement) within thirty (30) days after the due date specified in Section 16.2.1 of the Agreement for such payment and the failure by the County to cure such breach within thirty (30) days after the County has received written notice of such breach; or

b) a material breach by the County of any of its obligations under the Agreement and (A) the failure by the County to cure such breach within thirty (30) days after the County has received written notice of such breach; or (B) if the failure is not one that could reasonably be corrected within thirty (30) days, (1) the failure by the County to adopt, within thirty (30) days after receiving notice of such breach, a plan to cure any continuing breach within a time period not longer than sixty (60) days after the County received notice of the breach, or (2) the failure of the County to cure any continuing breach within such sixty (60)-day period.

73. DEFICIENCY(IES)

"Deficiency(ies)" shall mean outages, breakdowns, malfunctions, crashes or other loss or degradation of functionality.

74. DEMAND BATCH JOBS

"Demand Batch Jobs" shall mean batch jobs submitted by End-Users or Contractor's personnel.

75. DESIGNATED EMPLOYEES

"Designated Employees" shall mean those employees of the County, Legacy Provider and Subcontractors of Legacy Provider identified as such on a separate document delivered by the County to Contractor.

76. DESKTOP APPLICATION

"Desktop Application" shall mean Software that must execute on the desktop and that has a desktop footprint only, with no server component (e.g., Excel, Word, PowerPoint, etc.).

77. DESKTOP COMPUTING SERVICES

"Desktop Services" shall mean the Services described in Section 4.5 of Schedule 4.3-Operational Services.

78. DEVELOPMENT

"Development" shall mean the tasks necessary to provide new functionality which includes planning/analysis, design, build, test and deployment.

79. DISABLING DEVICE

"Disabling Device" shall have the meaning given to it in Section 7.1 of the Agreement.

80. DISENTANGLEMENT

"Disentanglement" shall have the meaning given to it in Section 6.1 of the Agreement.

81. DISENTANGLEMENT SERVICES

"Disentanglement Services" shall have the meaning given to it in Section 6.3 of the Agreement.

82. EFFECTIVE DATE

"Effective Date" shall mean November 15, 2016.

83. END-TO-END RESPONSE TIME

"End-to-End Response Time" shall mean the total elapsed time for a discrete data packet (for example, ping) to complete a round trip traversal of the computing infrastructure from a user interface device to a specific computing device resource and return. This shall exclude any local processing overhead time that may result from any County or Third-Party computing resources over which the Contractor has minimal control.

84. END-USER OR USER

"End-User" or "User" shall mean any County employee, or any other Person, who is determined by the County, in its sole discretion, to require access to any of the Services.

85. END-USER SERVICES

"End-User Services" shall mean the Services described in Section 3 of Schedule 4.3-Operational Services.

86. ENVIRONMENTAL LAWS

"Environmental Laws" shall mean all applicable federal, state, or local statutes, laws, regulations, rules, ordinances, decrees, codes, licenses, orders, permits or court decisions (including the so-called "common law"), including but not limited to, the Resource Conservation and Recovery Act, relating to hazardous substances, hazardous materials, toxic substances, environmental conditions or other similar substances or conditions including, but not limited to: (i) the Clean Air Act (42 U.S.C. 7401 et seq.); the Federal Water Pollution Control Act (33 U.S.C. §1251); the Safe Drinking Water Act (42 U.S.C. §5 300f et seq.); the Toxic Substances Control Act (15 U.S.C. 55 2601 et seq.); the Endangered Species Act (16 U.S.C. §1531 et seq.); the Emergency Planning and Community Right-to-Know Act of 1986 (42 U.S.C. 55 110011 et seq.); and (ii) similar state and local provisions.

87. EXCEPTION REPORT

"Exception Report" shall have the meaning given to it in Section 9.10.2 of the Agreement.

88. EXPIRATION DATE

"Expiration Date" shall have the meaning given to it in Section 6.2 of the Agreement.

89. FAILURE

"Failure" shall mean Contractor's failure to meet a Critical Milestone or Service Level.

90. FEE REDUCTION

"Fee Reduction" shall have the meaning given to it in Schedule 16.8.

91. FEES

"Fees" shall mean the fees payable by the County to Contractor hereunder in consideration of Contractor's provision of the Services.

92. FINAL ACCEPTANCE

"Final Acceptance" shall have the meaning given to it in Section 9.10.3 of the Agreement.

93. FINAL ACCEPTANCE CRITERIA

"Final Acceptance Criteria" shall have the meaning given to it in Section 9.10.3 of the Agreement.

94. FINAL ACCEPTANCE REVIEW PERIOD

"Final Acceptance Review Period" shall have the meaning given to it in Section 9.10.3 of the Agreement.

95. FINAL ACCEPTANCE REVIEW PROCEDURES

"Final Acceptance Review Procedures" shall have the meaning given to it in Section 9.10.3 of the Agreement.

96. FORCE MAJEURE EVENT

"Force Majeure Event" shall mean an act of God, act of governmental body or military authority other than a County governmental body, fire, explosion, power failure, flood, epidemic, riot or civil disturbance, war, sabotage, accidents, insurrections, blockades, embargoes, storms, labor disputes, or similar event beyond the reasonable control of the non-performing Party. Notwithstanding the foregoing, "Force Majeure Event" expressly excludes the following: any event that Contractor could reasonably have prevented by testing either required to be performed pursuant to the Services or necessary to provide the Services, work-around, or other exercise of diligence; any event resulting from any strike, walkout, or other labor shortage that could have been prevented by a reasonable amount of automation of functions; and any failure of any systems, facilities, or hardware that could have been prevented by testing either required to be performed pursuant to the Services or necessary to provide the Services.

97. FRAMEWORK COMPONENT

"Framework Component" shall mean a set of requirements for a specific functionality within a Service Framework and typically applies to a Resource Unit.

98. GAAP

"GAAP," is the acronym for "generally accepted accounting principles."

99. GOVERNMENT APPROVALS

"Government Approvals" shall mean such permits, waivers, approvals, or consents as are required, under applicable laws and regulations, in connection with the consummation and performance of

a particular agreement, event, or transaction, including the consummation and performance of this Agreement.

100. HAZARDOUS MATERIALS

"Hazardous Materials" shall mean any chemical, compound, material, substance or other matter that: (a) is a flammable, explosive, asbestos, radioactive nuclear medicine, vaccine, bacteria, virus, hazardous waste, toxic, overtly injurious or potentially injurious material, whether injurious or potentially injurious by itself or in combination with other materials; (b) is controlled, referred to, designated in or governed by any Environmental Laws; (c) gives rise to any reporting, notice or publication requirements under any Environmental Laws, or (d) is any other material or substance giving rise to any liability, responsibility or duty upon the County with respect to any third person under any Environmental Laws.

101. HARDWARE

"Hardware" shall have the same meaning as the term "Machines."

102. HIGH RESPONSE END-USER

"High Response End-User" shall mean End-Users who will receive immediate escalation for any Incident on a 24/7/365 basis. High Response End-Users shall designated in the Standards and Procedures Manual,

103. IMMEDIATELY

"Immediately" whether capitalized or not throughout the Agreement, shall mean a response where time is of the essence and instant action is required.

104. INCIDENT

"Incident" shall mean a reported perceived defect. Incidents shall be classified by Severity as described in Schedule 4.8.

105. INCLUDING

"Including" shall have the meaning given to it in Section 24.5 of the Agreement.

106. INFRASTRUCTURE SERVER

"Infrastructure Server" shall mean any Server other than an Application Server.

107. INFRINGEMENT CLAIM

"Infringement Claim" shall have the meaning given to it in Section 22.1 of the Agreement.

108. INITIAL TERM

"Initial Term" shall have the meaning given to it in Section 17.1.1 of the Agreement.

109. INSTALL

"Install" shall mean providing a new device to an existing County Site.

110. INTELLECTUAL PROPERTY RIGHTS

"Intellectual Property Rights" means all intellectual and industrial property rights, and similar or analogous proprietary rights including, but not limited to:

(i) patent rights (including, as applicable, the rights to make, use, sell, offer to sell, import into the United States, or have made, and the rights to file and prosecute patent applications and provisional patent applications);

(ii) rights associated with works of authorship, including copyrights and mask work rights (including the rights to copy, adapt, distribute, display, perform, and create derivative works);

(iii) rights relating to the protection of trade secrets and confidential information (including the rights to use and disclose);

(iv) trademarks, service marks, trade dress, trade names, and design patent rights (including the right to goodwill appertaining thereto);

(v) "moral rights"; and

(vi) other rights analogous, similar, or comparable to those described by the foregoing clauses (i) through (v), and other proprietary rights relating to intangible property (including licensing rights and shop rights).

111. IT

"IT" shall mean information technology.

112. KEY SUBCONTRACTORS

"Key Subcontractors" shall mean those Persons identified as such in Schedule 14.1.

113. KNOWN DEFECT

"Known Defect" shall mean a Deficiency in contracted-for functionality that is discovered/known prior to deployment (may be subject to warranty provisions).

114. LARGE WORK REQUEST

"Large Work Request" shall mean a Service Request for new Services where the total, recurring and non-recurring cost to the County is greater than $50,000.00.

115. LATENT DEFECT

"Latent Defect" shall mean a Deficiency in contracted-for functionality that is undiscovered/unknown prior to deployment (may be subject to warranty provisions) or a Contractor operationally induced error (e.g., file corruption).

116. LEGACY PROVIDER

"Legacy Provider" shall mean the County's IT and telecommunications outsource provider (including such provider's Subcontractors of any tier) providing Services to the County immediately prior to the Cutover Date of the applicable Service Framework.

117. LEVEL OF EFFORT (LOE) WORK REQUEST

"Level of Effort (LOE) Work Request" shall mean a Service Request for Services where the preponderance of the day-to-day work direction is provided by the County.

118. LOCAL AREA NETWORK OR LAN

"Local Area Network" or "LAN" shall mean the network connecting Desktop Computing Assets and other devices in a relatively small geographical area, such as a Site.

119. LOCATION

"Location" shall mean any present or future location at which the County conducts its operations, including offices and facilities, and any other location where the County wishes to receive Services, as specified by the County to Contractor at any time during the Term of the Agreement. The Locations include the Sites and the County Facilities. Location also includes any present or future location from which Contractor provides Services to the County.

120. LOSSES

"Losses" shall mean all losses, liabilities, damages, fines, claims (including taxes), mechanics' liens, other liens, awards and penalties, and all related costs and expenses (including reasonable legal fees and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties).

121. MACHINES

"Machines" means computers and related equipment, including laptop computers, desktop computers, central processing units and other processors, mainframes, telephones, mobile devices, tablets, services, controllers, modems, projectors, communications or telecommunications equipment, cables, circuits, storage devices, printers, scanners, terminals, other peripherals and input and output devices, and other tangible mechanical and electronic equipment intended for the processing, input, output, storage, transmission, and retrieval of information and data or voice communications. "Machines" also includes any data, and the tangible media used to support any of the foregoing, and all supporting documentation, media, and related materials, including written maintenance agreements, service agreements, license agreements, equipment lease agreements, Subcontractor agreements, and support documentation such as configuration documents and runbooks."

122. MANAGEMENT COMMITTEE

"Management Committee" shall mean the body described in Section 10.3 of the Agreement.

123. MAXIMUM ANNUAL FEE

"Maximum Annual Fee" shall mean the maximum amount payable under the Agreement in each Contract Year by the County to Contractor, as specified in Section 16.1.4 of the Agreement and Schedule 16.1.

124. MEASUREMENT PERIOD

"Measurement Period" means the period in which a given Service Level is measured (e.g., one month, one year).

125. MEDIUM WORK REQUEST

"Medium Work Request" shall mean a Service Request for new Services where the total, recurring and non-recurring cost to the County is greater than $15,000.00 and less than or equal to $50,000.00.

126. MIDDLEWARE

"Middleware" shall mean software that serves as a data-passing intermediary between Operating System Software and an Application. The term is also used to describe separate products that serve as the glue between two Applications; distinct from import and export features that may be built into one of the Applications.

127. MILESTONE

"Milestone" shall mean a point in a project plan when completion of a significant component or module is to be completed. Typically, Milestones are expressed as deliverables to the County in a Service Request.

128. MINIMUM PERFORMANCE

"Minimum Performance" shall mean the percentage of time or instances that a target SL must be met as specified in the applicable SL.

129. MISSION / BUSINESS CRITICAL

"Mission / Business Critical" shall mean Severity 2 Incidents as defined in Schedule 4.8.

130. MONTH

"Month" shall mean any calendar month during the Term of the Agreement.

131. MONTHLY SERVICES CHARGE (MSC)

"Monthly Services Charge" or "MSC" shall mean the charge to the County for Contractor's provision of all of the Services for any month during the Term.

132. MOVE

"Move" shall mean the relocation of an existing device from one County Site to another or within a County site.

133. NET BOOK VALUE (NBV)

For purchased assets, the Net Book Value of the asset is defined as the initial purchase price of the asset, excluding administrative cost and profit, less accumulated depreciation. For leased assets, the Net Book Value of the asset is defined as the value of all lease payments, excluding administrative cost and profit, less accumulated depreciation. Depreciation is calculated on a straight line, with asset life as defined as the County's contractual payment period for that asset as defined in Schedule 4.3. For example: desktop depreciation is over a life of 4 years and laptop depreciation is over a life of 3 years.

134. NETWORK SERVICES

"Network Services" shall mean the Services described in Section 5 of Schedule 4.3 – Operational Services.

135. NO DEFECT

"No Defect" shall mean an Incident when there is 1) no defect, or 2) an End-User induced error, or 3) password reset, End-User requested file restorations, etc.

136. ONLINE TRANSACTION RESPONSE TIME

"Online Transaction Response Time" shall mean the amount of time required to refresh End-User screen from point that enter command is given from End-User device.

137. OPTIONAL ITEM CATALOG OR OIC

"Optional Item Catalog" or "OIC" shall mean the on-line catalog used by the County to procure items as well as training services that are supported and/or provided by the Contractor, as specified in Schedule 16.1 of the Agreement.

138. PARTY

"Party" shall mean the County or Contractor, as applicable; "the Parties" shall mean each of the County and the Contractor.

139. PERFORMANCE TARGET

"Performance Target" shall mean the desired level of service County is seeking for a particular Service Level requirement.

140. PERSON

"Person" shall mean any natural person, corporation, limited liability company, limited liability partnership, general partnership, limited partnership, trust, association, governmental organization or agency, political subdivision, body politic, or other legal person or entity of any kind, legally constituted.

141. POINT OF PRESENCE (POP)

"Point of Presence" shall mean a network hub that connects many different networks or communications devices to provide End-Users access to the data center or Internet.

142. PLANNED OUTAGES

"Planned Outages" shall mean planned scheduled maintenance agreed to by the County and the Contractor.

143. PORTFOLIO APPLICATION LIST

"Portfolio Application List" shall mean the list of Portfolio Applications.

144. PORTFOLIO APPLICATIONS

"Portfolio Applications" shall mean non-Desktop Applications supported by the Contractor (excludes all Applications contained in the Optional Item Catalog).

145. PREMISES DEVICES

"Premises Devices" shall mean devices used by County End-Users to interface with the computing infrastructure, including workstations, Network attached printers and other Network attached peripherals.

146. PROBLEM

"Problem" shall mean any problem or circumstance that results from any of the following:

(i) an alleged Failure by either Party to perform its obligations under the Agreement;

(ii) an alleged inadequacy or delay of either Party's performance under the Agreement;

(iii) a request for products, services, or resources, where the Parties disagree whether such products, services, or resources are within the scope of the Agreement; or

(iv) a disagreement as to the responsibilities either Party has under the Agreement.

147. PROBLEM RESOLUTION REPORT

"Problem Resolution Report" or "PRR" shall mean a written report executed by both Parties describing a solution to a Problem, which terms will govern the behavior of the Parties until such time that the terms of the Problem Resolution Report are incorporated by amendment into the Agreement.

148. PROJECT

"Project" shall mean a temporary endeavor undertaken to create a unique product or service, or enhance an existing product, with varying levels complexity, risk, or integration.

149. PROJECT ESTIMATION

"Project Estimation" shall mean a set of disciplines and techniques that allow an IT professional to quantify labor and materials to determine schedule and cost, which is adjusted for risk. Project Estimation methods and tools provide a series of questions that allow the professional to input values to a system. The system provides a common frame of reference for the Contractor and County to understand how cost and schedule were derived.

150. PROVISIONAL TERMINATION DATE

"Provisional Termination Date" shall have the meaning set forth in Section 17.2.1 of the Agreement.

151. PUBLIC RECORD DATA

"Public Record Data" shall mean any "public record" as that term is used in the California Public Records Act.

152. PUBLIC SWITCHED TELEPHONE NETWORK (PSTN)

"Public Switched Telephone Network" or "PSTN" shall mean the network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.

153. PURCHASED ASSETS

"Purchased Assets" shall mean those Assets, including Machines, equipment, leases, licenses and other tangible and intangible property to be purchased by, assigned to or otherwise transferred to Contractor as of the Cutover Date for each applicable Service Framework, as set forth in a separate

document delivered by the County to Contractor before or concurrently with the Signing Date, and as updated by mutual agreement of the Parties (which agreement shall not be unreasonably withheld) at the Cutover Date for each applicable Service Framework, and such other property relating to the Services as may be identified by either Party in a written notice delivered to the other Party after the applicable Cutover Date and mutually agreed (which agreement shall not be unreasonably withheld) to be a Purchased Asset.

154. QUALITY

"Quality" shall mean a measurement based on counting the function points developed during a project and capturing the number of defects introduced into the User Acceptance testing environment that were specifically due to code or incorrectly applied configuration.

155. REMOTE ACCESS REQUEST FORM (RARF)

"Remote Access Request Form" or "RARF" shall mean a Service Request form used to request remote access to the County Network.

156. REMOVE

"Remove" shall mean taking an existing device or Desktop Application out of service from a County Site or End-User

157. REPORTING INTERVAL

"Reporting Interval" shall mean the time span between regular performance Reporting Periods.

158. REPORTING PERIOD

"Reporting Period" shall mean on a monthly basis, within three business days of the close of the calendar month, unless stated otherwise.

159. REQUEST FOR NETWORK ACCESS (RFNA) FORM

"Request for Network Access (RFNA) Form" shall mean a Service Request form used to request access to County Applications from non-Contractor assets.

160. REQUIRED CONSENTS

"Required Consents" shall mean Government Approvals and other Third-Party consents or approvals required in connection with:

(i) the assignment to and assumption by Contractor of the Assigned Contracts and Assigned Leases;

(ii) the licensing, granting, or transferring to Contractor of the right to use, access, and (if necessary) modify any of the Retained Assets, County Software, and any of the assets and properties covered by any of the Retained Assets, in connection with Contractor's performance of the Services;

(iii) the assignment to and assumption by the County of the Assigned Contracts and Assigned Leases in connection with Disentanglement;

(iv) the performance of the Services under the Agreement.

161. RESIDUALS

"Residuals" shall mean Contractor's general knowledge, skill, and experience, any ideas, concepts, know-how, and technologies that are within the scope of Contractor's business practice and are used, acquired, or developed by it in the course of providing the Services; provided, however, that the Residuals shall not include any Work Product or any of the County's Confidential Information.

162. RESOLVE

"Resolve" shall mean to repair, replace, reconfigure, re-install, reroute, or otherwise provide a complete solution to an Incident that returns the System and/or End-User(s) to non-degraded full

functionality. A Workstation Incident at a virtual office/remote access (VORA) site is considered "Resolved" by the overnight shipment of a repaired or a replacement Workstation that is fully operational. Implementing a Workaround is a partial or temporary resolution.

163. RESPOND TIME (TIME TO RESPOND)

"Respond Time" or "Time to Respond" shall mean the duration between when an Incident is reported to the Contractor and when a Contractor support technician or engineer provides initial feedback to County.

Calculation: Performance = Actual time to respond/target time to respond.

164. RESOURCE UNIT (RU)

"Resource Unit" or "RU" shall mean a particular unit of utilization of resources that have a Baseline Volume, as described in Schedule 16.1, and that is measured to determine the County's actual utilization of such resource for the purposes of calculating the Fees in accordance with Schedule 16.1.

165. RESOURCE UNIT FEE

"Resource Unit Fee" shall have the meaning set forth in Schedule 16.1.

166. RESOLVED

"Resolved" shall mean that a Problem or Incident is corrected to the County's satisfaction or back to the intended functionality of a system.

167. RESPONSE TIME OF THE APPLICATION

"Response Time of the Application" shall mean the elapsed time from when the "return" key is pressed to the response back to the screen, fully refreshed by the Application. Sometimes, this is called End-to-End response time. The Contractor will be responsible for this metric if it has responsibility for all components of the systems and network.

168. RETAINED ASSETS

"Retained Assets" shall mean the Software, Hardware and other assets (including their related written maintenance agreements, service agreements, Software license agreements, equipment lease agreements and Subcontractor agreements to which the County or the State is a party), that are not assigned to or not otherwise owned or leased by Contractor or any Subcontractors yet managed and administered by Contractor pursuant to Schedule 4.3. A list of the Retained Assets shall be included in the Standards and Procedures Manual, and shall be updated from time to time by the Parties. "Retained Assets" shall include Retained Desktop Computers.

169. RETAINED DESKTOP COMPUTERS

"Retained Desktop Computer" shall mean Retained Assets that are devices defined in the Desktop Computing Component in Section 4 of Schedule 4.3.

170. RETIREMENT

"Retirement" shall mean the work required to take an Application permanently out of service. Such work shall be performed solely pursuant to a Service Request.

171. ROOT-CAUSE ANALYSIS

"Root-Cause Analysis" shall mean the Problem analysis process described in Section 4.9 of the Agreement.

172. SALES TAX(ES)

"Sales Tax(es)" shall have the meaning given to it in Section 16.5 of the Agreement.

173. SCHEDULED MAINTENANCE

"Scheduled Maintenance" shall mean preventative, Decommission, Retirement, or planned Software updates.

174. SCHEDULED TIME

"Scheduled Time" shall mean the time during which Service is to be operational as designated in the applicable Service Level table. All references to schedule (for example, 0730 hours) in the Service Level tables are local time for the point of service.

175. SCHEDULED UPTIME

"Scheduled Uptime" shall mean the required System Availability that excludes all Planned Outages.

176. SEI/CMM LEVEL

"SEI/CMM Level" shall mean the Software Engineering Institute/Capability Maturity Model that is a reference model used for determining a software development organization's level of competency. Level 1 is characterized by an organization's ad-hoc development processes; Level 2 has repeatable processes; Level 3 has defined or documented processes that are consistently used; Level 4 has metrics for managing the processes, and Level 5 includes processes for optimization and improvement.

177. SERVERS

"Servers" shall mean all server classes defined (e.g., Infrastructure Server, Application Development Server, Application Pre-Production Server, Application Test Server and Application Production Server).

178. SERVICE DESK SERVICES

"Service Desk Services" shall mean the Services described in Section 2 of Schedule 4.3.

179. SERVICE FRAMEWORK

"Service Framework" shall mean any one or more of the following categories of Services described in Schedule 4.3: (1) Cross Functional Services, (2) Service Desk Services, (3) End-User Services, (4) Network Services, (5) Data Center Services, and (6) Application Services.

180. SERVICE LEVEL (SL)

"SL," which is the acronym for "Service Level," shall mean the minimum functional and operational performance levels specified in Schedule 4.8 for any task or service.

181. SERVICE PORTAL

"Service Portal" shall mean a secure website planned, built and operated by Contractor that resides on the County Intranet that provides End-User access to centralized IT and Telecommunications services and content in accordance with requirements in Schedule 4.3.

182. SERVICE REQUEST

"Service Request" shall mean End-User authorized request for Services in accordance with requirements in Schedule 4.3.

183. SERVICES

"Services" shall mean all services, functions and activities to be provided by Contractor under the Agreement, including, but not limited to, all of the following:

(i) Current Services;

(ii) The services described in Schedule 4.3;

(iii) Any services described in the Agreement that can be performed by Contractor's, or its Subcontractor's, personnel falling into any of the Application Services Labor categories listed in Exhibit 16.1-4 of Schedule 16.1;

(iv) Any other services specified elsewhere in the Agreement;

(v) Any other IT-related services that are requested by the County from time to time during the Term; and

(vi) Any procurement, maintenance, support, design, management, planning, and other services that are incidental, ancillary, customary, or necessary to and appropriate for the performance and receipt of any of the foregoing, exclusive, however, of services or functions for which the County expressly retains responsibility under the Agreement.

184. SHARED RESOURCES

"Shared Resources" shall have the meaning given to it in Section 7.6 of the Agreement.

185. SITE

"Site" shall mean each physical Location to which or from which Contractor provides the Services. The term "Site" is more fully defined in Schedule 4.3, Section 5.16.2.

186. SOFTWARE

"Software" means computer programs and program objects of any kind (including object code, source code, service and any intermediate forms or versions thereof), program set up and customization parameters and data, and the tangible media on which any of the foregoing are recorded, and all supporting documentation, media, written maintenance agreements, service agreements, license agreements, equipment lease agreements, Subcontractor agreements, and support documentation such as configuration documents and runbooks, and any other related documentation. When used individually, includes County Software, Contractor Software and Third-Party Software.

187. SPECIFICATIONS

"Specifications" shall mean the functional and technical requirements of a solution, which are codified in a document.

188. STANDARDS AND PROCEDURES MANUAL (SNP MANUAL)

"Standards and Procedures Manual" or "SnP Manual" shall mean the written manual developed by Contractor as described in Section 7.3 of the Agreement.

189. STATE

"State" shall mean the State of California.

190. SUBCONTRACTOR

"Subcontractor" shall mean any Person (including any Contractor Affiliate), other than Contractor, that provides Services, directly or indirectly, to the County pursuant to an agreement with (i) Contractor or (ii) a Subcontractor (of any tier) of Contractor. The term Subcontractor shall not include suppliers of Hardware and Software where the Person supplies only Hardware or Software and directly related maintenance and support services.

191. SYSTEM

"System" means the combination of the infrastructure, Middleware, and the Application or Applications Suite.

192. SYSTEM OF RECORD

"System of Record" means a production system that has been recognized by the County as the official basis for business transactions.

193. TARGET

"Target" shall mean the desired level of service County is requiring for a particular Service Level metric.

194. TASK-BASED SERVICE REQUEST

"Task Based Service Request" shall mean a Service Request for services where the preponderance of the work is pre-defined and results in deliverable products.

195. TERM

"Term" shall mean the period during which Contractor shall be obligated to provide the Services, as specified in Section 17.1 of the Agreement.

196. TERMINATED SERVICES

"Terminated Services" shall mean any Service, category of Service, or any discrete component, deliverables, features, functions, capabilities, tasks, activities, or portion of the Services, that Contractor and/or any Subcontractors shall cease performing under the Agreement and that may be assumed by the County, or by any Third-Party provider designated by the County.

197. TERMINATION DATE

"Termination Date" shall have the meaning given to it in Section 17.2.1 of the Agreement.

198. TERMINATION NOTICE

"Termination Notice" shall have the meaning given to it in Section 17.2.1 of the Agreement.

199. THIRD-PARTY

"Third Party" is i) a Person who provides Hardware, Software or other Services to the County and that is not a Subcontractor, or ii) a non-County Person to whom County directs Contractor to

provide Contractor Services as a result of a Service Request, or iii) a non-County Person with whom the County directs Contractor to create an interface or other connectivity with the County.

200. THIRD-PARTY RESOURCES

"Third-Party Resources" shall have the meaning given to it in Section 4.6 of the Agreement.

201. THIRD-PARTY SOFTWARE

"Third-Party Software" means Third-Party Works comprising Software and all supporting documentation, media, and related materials, provided or made available to the County by Contractor through its Subcontractors or other third parties or otherwise used by Contractor or its Subcontractors in connection with the performance of the Services (and all updates, enhancements, customizations, and other improvements thereof).

202. THIRD-PARTY WORKS

"Third-Party Works" means Underlying Works conceived, invented, created, or acquired by a Third-Party.

203. TICKET

"Ticket" shall mean the mechanism for recording Incidents in the Contractor's Service Desk systems.

204. TRANSITION

"Transition" shall have the meaning given to it in Section 2.1, of the Agreement.

205. TRANSITION PLAN

"Transition Plan" shall mean the plan described in Section 2.1, a copy of which is attached hereto as part of Schedule 2.1, of the Agreement.

206. TRANSITIONED EMPLOYEE

"Transitioned Employee" shall mean each Designated Employee who accepts an offer of employment from Contractor or a Subcontractor and becomes an employee of Contractor or a Subcontractor pursuant to this Agreement.

207. UNDERLYING WORKS

"Underlying Works" means tangible and intangible information and developments that: (i) had already been conceived, invented, created, developed or acquired by Contractor or Third-Parties prior to the Effective Date and were not conceived, invented, created, developed or acquired for the County's use or benefit in connection with this Agreement; or (ii) were conceived, invented, created, developed or acquired by Contractor or Third-Parties on or after the Effective Date, but only to the extent such information and developments do not constitute Work Product hereunder. An Underlying Work includes all intermediate and partial versions thereof, including all source code and object code with respect thereto, and all processes, methods, apparati, programs, procedures, designs, specifications, inventions, discoveries, improvements, ideas, know-how, techniques, materials, program materials, Software, flow charts, notes, outlines, lists, compilations, manuscripts, writings, reports, data, data models, pictorial materials, schematics, other creations, and the like, whether or not patented or patentable or otherwise protectable by law.

208. UNIX SERVER

"UNIX Server" shall mean any Server running the UNIX Operating System (e.g., Solaris, HP-UX, Tru64, AIX).

209. UNSCHEDULED MAINTENANCE

"Unscheduled Maintenance" shall mean unplanned maintenance to resolve defects.

210. VOICE SERVICES

"Voice Services" shall mean those Services described in Section 5 of Schedule 4.3 – Operational Services.

211. VOICE SWITCH OR PBX

"Voice Switch or PBX" shall mean a Voice Switch (also known as a PBX (Private Branch Exchange)), which is an electronic system capable of switching, routing, and connecting internal voice callers to each other as well as to external telephone lines. The PBX provides a switching matrix that allows internal telephones within an organization to:

- connect to other internal telephones
- connect to external telephone lines to make voice calls to "outside" telephones
- receive incoming telephone calls from "outside" callers.
- record calling data in order to charge users for the cost of toll calls.

In addition, a PBX provides hundreds of call handling and processing features that allow users to control, direct, route, and process incoming and outgoing telephone calls in a manner best suited to meet their business call processing needs. This ranges from such common items as call forwarding, transfer, restriction, direct dial to more sophisticated capabilities such as automatic call distribution and alternative routing.

212. WARN ACT

"WARN Act" means the Worker Adjustment and Retraining Notification Act, 29 U.S.C. §§ 2101 et seq, and any state or local statute, code, regulation or ordinance that is analogous or similar to the WARN Act.

213. WARN NOTICE

"WARN Notice" means a notice required by the WARN Act, or other applicable law, to be provided to a Party's (including Subcontractor's) employees in connection with an event or circumstance that is likely to result in the termination or redeployment of such employees and that might result in the imposition of incremental severance and other costs, damages, fines, or penalties if such laws are not fully complied with.

214. WEEK

"Week" shall mean a week of seven (7) days, Sunday through Saturday, including County holidays.

215. WEIGHTING FACTOR

"Weighting Factor" shall have the meaning set forth in Schedule 16.8.

216. WIDE AREA NETWORK OR WAN

"WIDE AREA NETWORK" or "WAN" shall mean a network linking together networks located in other geographical areas.

217. WORK PRODUCT

"Work Product" means all tangible and intangible information and developments, and intermediate or partial versions thereof, including source code and object code with respect thereto, and all processes, methods, apparati, programs, procedures, designs, specifications, inventions, discoveries, improvements, ideas, know-how, techniques, materials, program materials, Software, flow charts, notes, outlines, lists, compilations, manuscripts, writings, reports, data, data models, pictorial materials, schematics, other creations, and the like, whether or not patented or patentable, subject to copyright, constituting a trade secret, or otherwise protectable by law, that are conceived, invented, created, developed or acquired by Contractor in its performance under this Agreement, or by any Person engaged by Contractor in the performance of Contractor's obligations or the

exercise of Contractor's rights under this Agreement, and the Intellectual Property Rights in or pertaining to any of the foregoing.

218. WORKSTATION

"Workstation" shall mean an End-User computing device, ranging in power and function from a desktop or laptop PC to a high end engineering or graphic workstation.

END OF SCHEDULE

Appendix A-2 – Assigned Contracts

Contractor shall provide a list of Assigned Contracts to County on or before the completion of Transition of Applications Services.

END OF SCHEDULE

Appendix A-3 – Assigned Leases

Contractor shall provide a list of Assigned Leases to County on or before the completion of Transition of Applications Services.

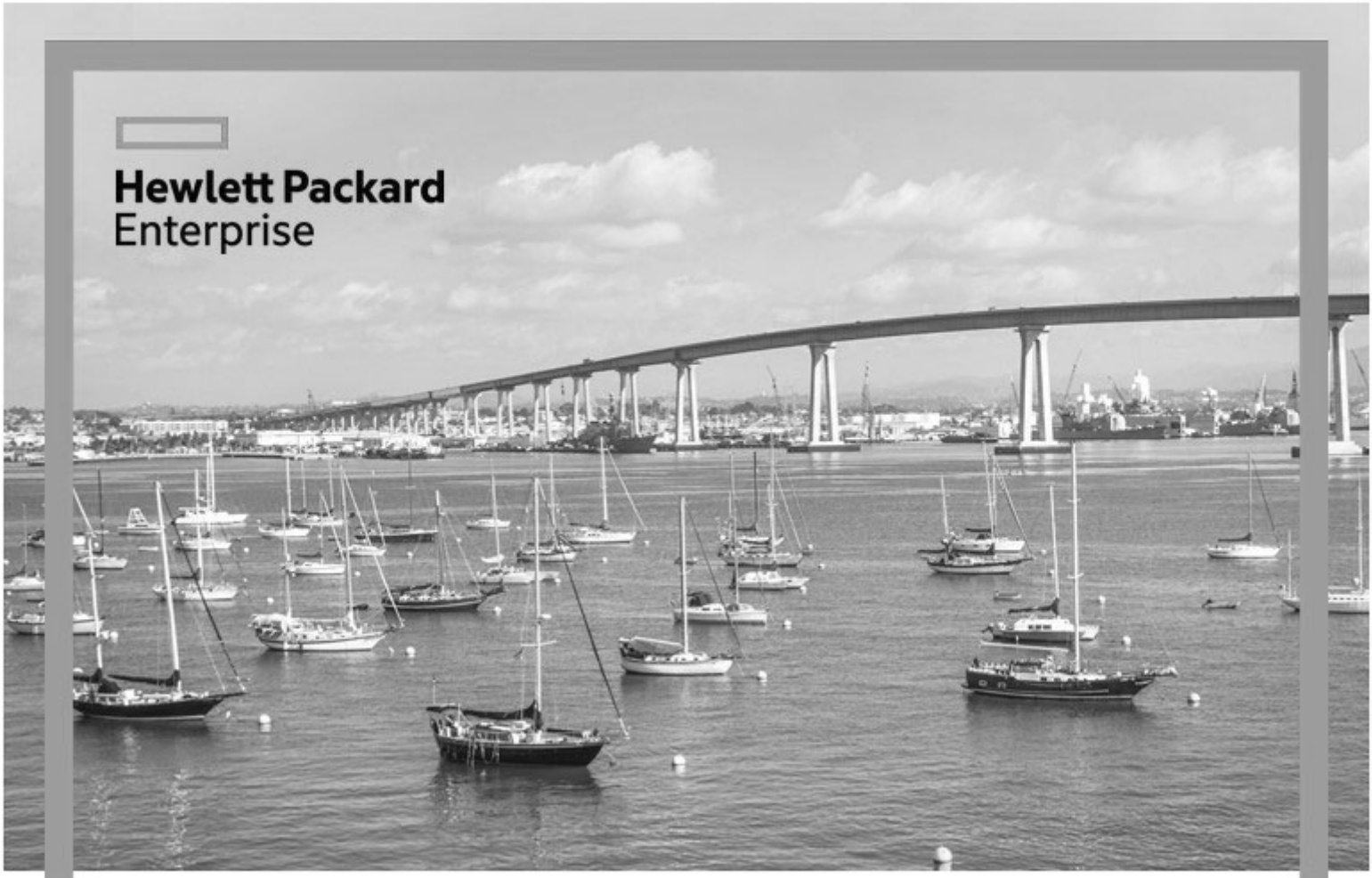
END OF SCHEDULE

Appendix A-4 – Contractor Software

Contractor shall provide a list of Contractor Software to County on or before the completion of Transition of Applications Services.

END OF SCHEDULE

Schedule 1.2 – Offeror's Proposal



Hewlett Packard
Enterprise

Driving Results

Committed, progressive partner moving the County forward through innovation and continuous improvement

HP Enterprise Services' Response to the County of San Diego Request for Proposals (RFP) 7189 – Information Technology & Telecommunications Services

Final Submission

October 2016

Volume I - Terms and Conditions

Executive Summary

In recent years, the County of San Diego has transformed the way residents and visitors receive valuable services, obtain information and interact with County officials. With successful efforts to provide digital government, mobility services, business continuity and workforce optimization, the County has been recognized as one of the nation's most technologically advanced counties, achieving numerous awards and accolades. Whereas recognition is notable, the beneficial impact to County employees, taxpayers and residents is what is truly impressive. HPES is proud to have been your partner over the past 10 years in this drive to achieve operational excellence.

HPES understands the County's mission to improve the lives of San Diegans through Safe Communities, Sustainable Environments, Healthy Families, and Operational Excellence. The technology foundation enabling the support of these initiatives relies on systems and services delivered and maintained by our team. Our approach and performance provides the County peace of mind that IT is being managed properly so you can focus on that noblest of motives, the public good.

We must also continue to address the challenges facing County residents, particularly those in danger of being disenfranchised, Veterans, foster children, the homeless, and those suffering from mental illness. We view our role in the County, not just in the context of technology, but as a key enabler to better business outcomes as you strive to "connect the unconnected."

San Diego County has a proud military heritage. Our team will implement programs to support military residents and returning Veterans. Working with groups such as Mission Edge San Diego (Three Wise Men), we will develop training programs tailored for military personnel with the goal of providing the technology skills required to be competitive in the job market.

The County has been successful in raising the "IT IQ" of County personnel. We embrace this concept and will, in collaboration with CTO and support from key providers like Adobe and Microsoft, deliver training programs for County personnel focused on transformative learning that will enable them to most effectively utilize the capabilities and functionality of software and services in which the County is investing.

Our approach to providing IT services to the County has always been to deliver the right solution at the best price, in line with County's strategic objectives. Our commitment is to build on that approach. We have strong relationships with top tier providers including EMC, Oracle and IBM. Whether a technology comes from a strategic partner or a perceived competitor, we will bring the best solution to the County to achieve the best business outcome. The delivery of reliable, predictable and quality results, with high end-user satisfaction, is of utmost importance to us. We are pleased to note that together with County CTO, we achieved the highest rating to date in the annual Gartner IT customer satisfaction survey, reaching the top category, "Best in Class".

Operational excellence requires the pursuit of continuous improvement. At all levels across our organization, our focus on problem solving, teamwork and leadership will ensure we consistently identify and seize opportunities to provide optimal results. The transformative specifics in our proposal provide mechanisms the County can leverage to foster new ways of thinking and spark creativity among our teams across the County, industry partners, and constituents. We will ensure a sound foundation from which the County can address current challenges as well as provide services to the next generation resident - one who is proactive, connected, and aspiring to contribute. Like the County, we believe that "Good Government Demands the Intelligent Interest of Every Citizen" and we will collaborate with the

County to identify and implement technologies and programs to encourage that interest, and enable every citizen to be engaged.

Building on the vision established by the CTO, HPES developed a local Innovation Council. The council's charter is to address real business needs, increase efficiency and reduce County spend. Once a year, we host Innovation Day at the COC for all interested County users where these innovation ideas are showcased. Since 2014, the Innovation Council has presented 26 ideas, 10 of which have been implemented into production. These solutions have had a positive impact on County users and citizen-centric services.

HPES is honored to be a Live Well San Diego partner. Our commitment to the community is also demonstrated through engagements like election night support, fielding a team for the Live Well San Diego 5K, sponsoring and attending the State of the County address, and providing speakers and technical support for County events such as Passport to Life Career & Education Expo and the Dick Wayman Technology Center Ribbon Cutting Ceremony at the Ramona Library. At numerous other County events you will find the employees of HPES and our partner AT&T in the mix; participating, supporting and occasionally sponsoring. We are engaged and involved on a personal level.

And for good reason: We live here. Our highly qualified team is primarily comprised of San Diego County residents. We understand what we do matters, to our families, our friends, our neighbors, and the entire San Diego region.

You will see many familiar names in our list of 20 Key Personnel; individuals who have worked shoulder to shoulder with the County delivering consistent results, solving problems and building a relationship of trust. The team will continue to be led by Cathy Varner, our current and proposed Account Executive, who has been supporting the County since 2006. Our telecommunications partner, AT&T, will continue to be led by Grant Morgan, who has also supported the County for 10 years. Together, our team has a broad set of skills uniquely suited to supporting the County. From architects and engineers to service desk and desk side support, we are steadfast in our commitment. We are knowledgeable of County business and culture and we demonstrate that knowledge in every aspect of our performance.

It has been a privilege for HPES to support the County's IT and Telecommunications for the past 10 years. We do not take for granted the trust the County has placed in us. Our core tenet has been and will continue to be, "we must earn the opportunity to do business with the County". As the incumbent, our knowledge and experience presents the lowest risk transition. We will continue to consistently deliver the County's IT operations while we transition and transform to the technologies required by the new scope of work and beyond.

The new frontier for our partnership will be a model of excellence in reliability, continuous improvement, transformation, and strategic alignment, advancing the gauge for County staff, constituents, and visitors.

As we move forward in our partnership, you can be assured that your reputation as the best managed local government in America will continue to be affirmed.

Volume I – Terms and Conditions

1.1 Cover Page (PC 600)

We have provided the required PC 600 on the following page as well as in an envelope as specified on the form.

SUBMITTAL INFORMATION	
Submit this Completed Form as the Cover Page of Your Proposal	
PROPOSAL DUE DATE: 05/02/2016; 3:00 PM local San Diego time	
Submit in a separate sealed envelope(s) or package(s) marked on the outside with "RFP 7189" to: County of San Diego Department of Purchasing and Contracting 5560 Overland Avenue, Suite 270 San Diego, CA 92123-1204	**For information, please contact:** Allen Hunsberger (858) 505-6362 cosd.purchasing@gmail.com

DESCRIPTION
The County of San Diego is soliciting proposals for Information Technology (IT) and Telecommunications Services

TO BE COMPLETED BY OFFEROR	
OFFEROR INFORMATION (Type or Print)	NAME, TITLE & CONTACT NUMBER OF PERSON AUTHORIZED TO SIGN OFFER (Type or Print)
HP Enterprise Services, LLC Offeror Company/Organization Name	Steve Tolbert Authorized Representative Name
16550 West Bernardo Drive, Building 2 Offeror Address	VP State Local and Education Authorized Representative Title
San Diego, CA 92127 Offeror City, State, Zip	steve.tolbert@hpe.com Authorized Representative Email Address
(858) 674 8600 Offeror Telephone Number	(703) 689 1265 Authorized Representative Telephone Number
www.hpe.com Offeror Website Address	
( ) Offeror Fax Number	

SIGNATURE	
I certify under penalty and perjury under the laws of the State of California, that I am authorized to execute and submit this proposal on behalf of the Offeror listed above; that all of the RFP instructions and rules, exhibits, addenda, questions and answers, and any other information provided by the County, including but not limited to, the diligence material, has been reviewed, understood and complied with; and that all information in this submission is true, correct, and in compliance with the terms of the RFP.	
Steve Tolbert Authorized Representative Signature	**November, 1, 2016** Date

1.2 Representations and Certifications

We have provided HPES' scanned, signed form, as required, on the following page.

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

County of San Diego
Department of Purchasing and Contracting

REPRESENTATIONS AND CERTIFICATIONS

The following representations and certifications are to be completed, signed and returned with the offer (the term "offer" includes bids, proposals, quotes or any other submission to provide goods and/or services).

1. **BUSINESS TYPE**
   ■ For-profit ☐ Non-profit ☐ Government
   Attach proof of status for Non-profit.
2. **INTERLOCKING DIRECTORATE**
   In accordance with Board of Supervisors Policy A-79, if Offeror is a non-profit as indicated in paragraph 1 above, Offeror is required to identify any related for-profit subcontractors in which an interlocking directorate, management or ownership relationship exists. If Offeror is a non-profit and will be subcontracting with a related for-profit entity, Offeror must list all such entity(ies) on an attached separate sheet, and authorization must be sought from Board of Supervisors. If Offeror is a non-profit and does not submit such a list, Offeror certifies it has no and will not enter into a subcontract relationship with a related for-profit entity.
3. **BUSINESS REPRESENTATION**
   Offeror represents as a part of this offer the following information regarding the ownership, operation, and control of its business:
   - **3.1.** Are you a local business with a physical address within the County of San Diego? ■ Yes ☐ No
   - **3.2.** Are you certified by the State of California as a:
     ☐ Disabled Veteran Business Enterprise (DVBE)
     Certification #: _____
     ☐ Small Business Enterprise (SBE)
     Certification #: _____
   - **3.3.** Are you certified by the U.S. Dept Of Veterans' Affairs as:
     ☐ Veteran Owned Small Business (VOSB)
     Certification # _____
     ☐ Service Disabled Veteran Owned Small Business (SDVOSB)
     Certification # _____
   - **3.4.** Estimated percentage of work in this offer to be performed or fulfilled locally (within the geographic boundaries of the County of San Diego): 65 %
4. **DEBARMENT, SUSPENSION AND RELATED MATTERS**
   - **4.1.** Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:
     - **4.1.1.** Are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency.
     - **4.1.2.** Have within a three (3) year period preceding this agreement been convicted of or had a civil judgment rendered against them for commission of fraud or criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
   - **4.2.** Except as allowed for in Section 4.2.4, Offeror hereby certifies to the best of its knowledge that neither it nor any of its officers:
     - **4.2.1** Are presently indicted for or otherwise criminally or civilly charged by a government entity (federal, state, or local) with the commission of any of the offenses enumerated in paragraph 4.1.2 of this certification;
     - **4.2.2** Have within a three (3) year period preceding this agreement had one or more public transactions (federal, state or local) terminated for cause or default;
     - **4.2.3** Are presently the target or subject of any investigation, accusation or charges by any federal, state or local law enforcement, licensing or certification body.
     - **4.2.4** If Offeror is unable to certify any of the facts set forth in Sections 4.2.1, 4.2.2 or 4.2.3, it certifies that is has listed on a separate sheet(s) attached to this Representations and Certifications each fact that it cannot certify and the reason it cannot do so. That information must include the specific relevant facts (date(s), contract(s) and individual(s) involved, status of action(s), and any other relevant information) that prevent it from making the requested certifications. The County reserves the right to disqualify an Offeror based upon information disclosed.
   - **4.3** Offeror has a continuing duty to disclose information until contract award/execution and shall report in writing to the County Department of Purchasing and Contracting within five business days of knowing or have any reason to know any change in status as certified in the preceding paragraphs 4.1 and 4.2.
   - **4.4** If Offeror or any of its subcontractors, agents or consultants, have previously contracted with the County to perform related work on this project (e.g. preparing components of the statement of work or plans and specifications for this project), Offeror shall identify those previous agreement(s) and submit that list along with the proposal. Other than as may be submitted on said list, Offeror certifies to the best of its knowledge that it and its proposed subcontractors, agents and consultants have not previously contracted with the County to perform work on or related to this project.
5. **CURRENT COST OR PRICING**
   Offeror certifies to the best of its knowledge that cost and/or pricing data submitted with this offer, or specifically identified by reference if actual submission of the data is impracticable, are accurate, complete, and current as of the date signed below.
6. **INDEPENDENT PRICING**
   Offeror certifies that in relation to this procurement:
   - **6.1.** The prices in this offer have been arrived at independently, without consultation, communication, or agreement, for the purpose of restricting competition, as to any matter relating to such prices with other offerors, with any competitors, or with any County employee(s) or consultant(s) involved in this or related procurements;
   - **6.2.** Unless otherwise required by law, the prices that have been quoted in this offer have not been knowingly disclosed by the Offeror and will not knowingly be disclosed by the Offeror prior to opening, in the case of a bid, or prior to award, in the case of a proposal, directly or indirectly to any other Offeror or to any competitor; and
   - **6.3.** No attempt has been made or will be made by the Offeror to induce any other person or firm to submit or not to submit an offer for the purpose of restricting competition.
7. **TAX INFORMATION**
   The Offeror understands that prior to receiving a contract award from the County, the Offeror must submit a completed IRS W-9 form to provide a Federal Tax ID number, or if not available, to provide a Social Security Number (SSN).

CERTIFICATION

The information furnished in Paragraphs 1 through 7 and in the accompanying offer is certified to be factual and correct as of the date submitted and this certification is made under penalty of perjury under the laws of the State of California.

Name: Steve Tolbert
Signature: Steve Tolbert
Title: VP State Local and Education
Date: 8/8/16
Company/Organization: HP Enterprise Services, LLC

SUBMIT THIS FORM AS DIRECTED IN THE REQUEST FOR SOLICITATION DOCUMENTS OR WITH THE OFFER

Revised 01-15-16

Page 16 of 25

In response to Section 4.2.2:

On August 28, 2015, the State of Michigan terminated its contract with HP Enterprise Services, LLC (HPES), for the design, build, and implementation of a Business Application Modernization platform for the Michigan Department of Motor Vehicles. HPES met multiple project milestones and delivered goods and services of value to the State as part of the project. A dispute arose between the State and HPES regarding project delays and the State's failure to pay HPES for services performed. HPES had been working in good faith to reach a business resolution of the parties' disagreements, but the State abruptly stopped negotiating and initiated litigation. HPES looks forward to a favorable resolution in court.

1.3 Nondisclosure Indemnification Agreement Form (page 17 of 25)

The Nondisclosure Indemnification Agreement Form is included on the following page.

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

NONDISCLOSURE INDEMNIFICATION AGREEMENT

IF OFFEROR SUBMITS EXHIBIT CONFIDENTIAL/PROPRIETARY, THE FOLLOWING NONDISCLOSURE INDEMNIFICATION AGREEMENT MUST BE COMPLETED, SIGNED AND RETURNED WITH THE OFFER

This indemnification agreement ("Agreement") is made and entered into by and between the County of San Diego ("County") and Offeror Company/Organization Name: HP Enterprise Services, LLC ("Offeror") with reference to the following facts:

WHEREAS the County may receive a request for disclosure of Offeror's submission under the California Public Records Act, Government Code Section 6250, et seq.; and

WHEREAS, Offeror has included in its submission an exhibit entitled "*EXHIBIT – CONFIDENTIAL/PROPRIETARY*" containing records that Offeror has determined to constitute trade secrets or other proprietary information exempt from disclosure under the California Public Records Act; and

WHEREAS the County requires defense and indemnity from Offeror for the County's ongoing non-disclosure of Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*;

NOW, THEREFORE, for good and valuable consideration and the mutual promises contained herein, the parties agree to the following:

1. The above recitals are incorporated herein by this reference.

2. Except as otherwise provided herein, the County will not release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* based on Offeror's representation that the records contained therein are proprietary and exempt from disclosure under the California Public Records Act and/or are trade secrets as that term is defined in Government Code Section 6250, et seq. Notwithstanding the foregoing, however, the County may release Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY* in the event of any of the following:

   a. Offeror fails to comply with the terms and conditions of this Agreement; or
   b. Offeror provides the County with written notice that some or all of the records may be released; or
   c. A court of competent jurisdiction orders the County to release the records and the County has exhausted or waived its appeal rights.

3. To the fullest extent allowed by law, the County shall not be liable for, and Offeror shall defend and indemnify County and its Board of Supervisors, officers, directors, employees and agents of County (collectively "County Parties"), against any and all claims, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees (whether incurred by County attorneys or attorneys employed by County) and court costs (hereinafter collectively referred to as "Claims"), related to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*.

4. Offeror waives any and all claims in law or equity and hereby releases the County Parties from any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs, which arise out of or are in any way connected to Offeror's *EXHIBIT-CONFIDENTIAL/PROPRIETARY*.

TO BE COMPLETED BY AN AUTHORIZED REPRESENTATIVE OF THE OFFEROR	
Offeror Company/Organization Name:	HP Enterprise Services, LLC
Authorized Representative Name:	Steve Tolbert
Authorized Representative Title:	VP State Local and Education
Signature:	Date: 8/8/16

1.4 DVBE Requirements and Forms

We have provided on the following pages our completed DVBE forms.

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

DVBE REQUIREMENTS AND FORMS

The County, as a matter of policy, encourages the participation of Disabled Veterans Business Enterprises (DVBE) through DVBE participation goals. County of San Diego, Board of Supervisors DVBE policy B-39a is found at http://www.sdcounty.ca.gov/cob/policy/index.html#. The County DVBE program recognizes the California State DVBE certification, which may be found at http://www.pd.dgs.ca.gov.

For this solicitation:

Bidder/Offeror (Offeror) must meet or exceed a 3% DVBE Subcontractor Participation goal or show a good faith effort to do so. Offeror must submit a DVBE Subcontractor Participation Summary and DVBE Subcontractor Participation Plan based on total pricing/payment schedule of proposal. If the DVBE Subcontractor Participation Plan does not show that Offeror has met or exceeded the 3% DVBE Subcontractor Participation goal, Offeror must provide Documentation of a Good Faith Effort. Offerors are encouraged to submit the Documentation of Good Faith Effort even if they have met or exceeded the 3% DVBE Subcontractor Participation goal in the event that all or part of the DVBE Subcontractor Participation Plan is determined to be ineligible. County reserves the right to request a Documentation of Good Faith Effort from any Offeror regardless of utilization calculated on the DVBE Subcontractor Participation Plan.

(Remainder of this page left blank)

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

DVBE PARTICIPATION SUMMARY

This DVBE Subcontractor Participation Summary is required to document Bidder's/Offeror's (Offeror) compliance with the DVBE participation goals set forth in Board Policy B-39a.

All Offerors must complete this section
Offeror: Hewlett Packard Enterprise Services, LLC
Offeror's Representative: Steve Tolbert / HPE VP State, Local and Education

Exemptions (complete only if Offeror qualifies for one of the exemptions below)

Offeror is exempt from DVBE Subcontractor Participation Requirements in accordance with Board Policy B-39a because Offeror is a:

- ☐ Government Agency
- ☐ Nonprofit Organization
- ☐ Small Business Enterprise (SBE), pursuant to Board Policy B-53
  State of California Certification #: _____
- ☐ Veteran Owned Business (VOB), pursuant to Board Policy B-53

  VOB status due to certification as a:

  - ☐ DVBE - State of California Certification #: _____
  - ☐ VOSB - U.S. VA Certification #: _____
  - ☐ SDVOSB - U.S. VA Certification #: _____

Offeror must provide additional supporting documentation upon request.

DVBE Compliance (complete if Offeror claimed no exemption above)

- ☒ Complete and attach DVBE Subcontractor Participation Plan
- ☐ Complete and attach Documentation of Good Faith Effort (optional if Offeror has met or exceeded 3% participation goal)

THIS FORM SHALL BE SUBMITTED WITH PROPOSAL ON THE DUE DATE

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

DVBE SUBCONTRACTOR PARTICIPATION PLAN

Offeror: Hewlett Packard Enterprise Services, LLC Offeror Representative: Cathy Varner

Project Title: County Technology Office Information Technology (IT) and Telecommunications Services

ITEM NO.	DESCRIPTION OF WORK, SERVICE OR MATERIAL	NAME, ADDRESS, TELEPHONE NUMBER AND CERTIFICATION NUMBER OF CERTIFIED DVBE TO BE USED	DOLLAR AMOUNT TO BE PAID THIS DVBE
1	Database Administrator Applications Developer	Name: CPH Enterprises Address: 2220 K Street Sacramento, CA 95816 Telephone #: 916-337-9443 Certification #: 1736463	$6,159,932
2	Applications Architect Applications Developer	Name: Fortuna Address: 1130 Iron Point Road Suite 140 Folsom, CA 95630 Telephone #: 916-458-0991 Certification #: 1785679	$6,130,612
3	Applications Developer Project Manager	Name: Global Blue DVBE Address: 3715 Atherton Road, Suite 2 Rocklin, CA 95765 Telephone #: 916-425-4866 Certification #: 1567640	$6,151,968
4	Database Administrator Applications Developer	Name: Cognetic Technologies Address: 29937 Robbie Lane, Vista, CA 92084 Telephone #:619-806-8117 Certification #:53595	$6,784,831
5	Applications Architect Applications Developer	Name: Stanfield Systems Address: 718 Sutter St. Suite 108 Folsom, CA 95630 Telephone #:916-358-7115 Certification #: 23905	$6,038,078
6	Project Manager	Name: Patricio Systems Address: PO Box 5275 El Dorado Hills, CA 95762 Telephone #:916-941-6791 Certification #:1612340	$3,910,470
7	Application Developer Application Test Developer	Name: Sumrall Solutions Address: 4524 Mapleplain Ave Elk Grove, CA 95758 Telephone #:916-427-3307 Certification #:33460	$3,784,095
		TOTAL AMOUNT TO CERTIFIED DVBE	$ $38,959,986

Use additional sheets if necessary. Compute utilization on last sheet.

Sheet 1 of 2 (complete if submitting more than one sheet)

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

COMPUTATION OF UTILIZATION AND COMPARISON WITH THE SUBCONTRACTOR PARTICIPATION GOAL	
Total Amount to Certified DVBE / Total Bid/Proposal x 100 = Percent of Utilization	Goal = 3%
$38,959,986/$1,298,666,215 x 100 = * 3.0% * HPES is committed to supporting our veterans and meeting the County's (at least) 3% DVBE participation goal. Our participation will ramp up in the first few years of the contract and may fluctuate from year to year but we will meet the 3% participation goal over the life of the contract.	Submit Documentation of Good Faith Effort if goal is not met.

THIS FORM SHALL BE SUBMITTED WITH PROPOSAL ON THE DUE DATE

Use additional sheets if necessary. Compute utilization on last sheet.

Sheet 2 of 2 (complete if submitting more than one sheet)

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

DOCUMENTATION OF GOOD FAITH EFFORT- Page 1 of 3

A. **List potential DVBEs** that the Offeror solicited for participation in this contract along with dates. Use additional sheets if necessary.

	Certified DVBE Firm	Date of Contact (Mail, Fax, Telephone, etc.)	Responded (Yes/No)
1.	SOURCE DIVERSIFIED INC	March 7, 2016- email	No
2.	GLOBAL BLUE DVBE INC.	March 7, 2016- email	Yes
3.	PATRICIO SYSTEMS	March 7, 2016- email	Yes
4.	SELECT GROUP INC	March 7, 2016- email	Yes
5.	TITANIUM COBRA SOLUTIONS LLC	March 7, 2016- email	No
6.	GEO COAST INC	March 7, 2016- email	No
7.	INTERACT COMPUTING ENTERPRISE	March 7, 2016- email	No
8.	CAVU CONSULTING, INC	March 7, 2016- email	Yes- declined
9.	FORTUNA BUSINESS MANAGEMENT CONSULTING	March 7, 2016- email	Yes
10.	BRIAN FITZGERALD RPE.DVBE	March 7, 2016- email	No
11.	EXPEDITIONARY TECHNICAL SOLUTIONS INC	March 7, 2016- email	No
12.	PAPERLESS KNOWLEDGE INC	March 7, 2016- email	Yes
13.	O'CONNOR CONSTRUCTION MANAGEMENT, INC.	March 7, 2016- email	No
14.	CRESTPOINT SOLUTIONS INC	March 7, 2016- email	No
15.	THE ESSENTIAL LINK	March 7, 2016- email	No
16.	CONTROL POINT	March 7, 2016- email	No
17.	CPH Enterprises, LLC	April 06, 2016 - email	Yes
18.	ADVANCED ONION INC	March 7, 2016- email	No
19.	WARRIOR SOLUTIONS	July 15, 2016 – email/phone	Yes - declined
20.	PATRIOT DVBE	July 15, 2016 – email/phone	No

Sheet 1 of 2 (complete if submitting more than one sheet)

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

DOCUMENTATION OF GOOD FAITH EFFORT- Page 2 of 3

	Certified DVBE Firm	Date of Contact (Mail, Fax, Telephone, etc.)	Responded (Yes/No)
21.	STANFIELD SYSTEMS	July 15, 2016 – email/phone	Yes
22.	SUMRALL SOLUTIONS	July 18, 2016 – email/phone	Yes
23.	CHARLES A FLEMING ENTERPRISES	July 18, 2016 – email	No
24.	POST CONSULTING	July 18, 2016 – email	No
25.	REED CONSULTING SERVICES	July 18, 2016 – email	No
26.	NATIX, INC	July 18, 2016 – email	No
27.	SILVERLINC	July 18, 2016 – email	No
28.	INTERACT COMPUTING ENTERPRISE	July 18, 2016 – email	No
29.	VETERAN VELOCITY	July 18, 2016 – email	No
30.	EXPEDITIONARY TECHNICAL SOLUTIONS	July 18, 2016 – email	No
31.	COGNETIC TECHNOLOGIES	July 18, 2016 – email	Yes
32.			
33.			
34.			
35.			
36.			
37.			
38.			
39.			
40.			

Sheet 2 of 2 (complete if submitting more than one sheet)

Page **23** of **25**

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

B. **DVBE Solicitations**

Solicitation Sample:
Offeror must attach a sample of the solicitation sent to certified DVBE firms. If phone contact was made, document conversation: date, time, contact person, and business opportunities discussed.

THIS FORM SHALL BE SUBMITTED WITH PROPOSAL ON THE DUE DATE

COUNTY OF SAN DIEGO – REQUEST FOR PROPOSALS (RFP) 7189
COUNTY TECHNOLOGY OFFICE
INFORMATION TECHNOLOGY (IT) AND TELECOMMUNICATIONS SERVICES

DOCUMENTATION OF GOOD FAITH EFFORT- Page 3 of 3

Identification of: (1) All DVBEs that submitted bids/proposals, (2) Nature of work/supplies/services offered that are not accepted, (3) Dollar amounts of the DVBEs bids/proposals not accepted, (4) Subcontractors and/or suppliers that will be used instead of the DVBEs, (5) Dollar amounts of these subcontractors and/or suppliers' bids/proposals, and (6) The reason for the bidder/offeror not accepting the DVBE's bid/proposal. Use additional sheets if necessary.

Name of DVBE (1)	Nature of Work (2)	DVBE Bids/Offer($) (3)	Subcontractor/ Supplier to be used (4)	Bid/Proposal Amount Accepted (5)	Reason Not Accepted (6)
GLOBAL BLUE DVBE INC.	Project Management, App Development	$6,151,968			
PATRICIO SYSTEMS	Project Management	$3,910,470			
WARRIOR SOLUTIONS	Project Management	NA	Patricio Systems Global Blue DVBE	$0	DVBE Declined
CAVU CONSULTING, INC	Systems Engineering Cyber Security	NA	Cognetech	$0	DVBE Declined to participate
Fortuna Business Management Consulting, Inc.	App Development App Architecture	$6,130,612			
CPH Enterprises, LLC	App Development Database Administration	$6,159,932			
Stanfield Systems	App Development App Architecture	$6,038,078			
Cognetech	Database Administrator App Development	$6,784,831			
Sumrall Solutions	App Development	$3,784,095			

Sheet_____of_____(complete if submitting more than one sheet)

THIS FORM SHALL BE SUBMITTED WITH PROPOSAL ON THE DUE DATE

Page **22** of **25**

We have provided on the following pages a copy of the solicitation that was sent to the identified DBVE companies as part of our DVBE solicitation effort.

Hewlett Packard Enterprise Vendor Solicitation

Request for Information

Hewlett Packard Enterprise Services, LLC (HPE) is seeking to obtain information to determine if your company is able to provide services listed below for an upcoming opportunity with an HPE Public Sector Client located in the San Diego, California, vicinity. Opportunities could require qualified vendors to support projects or operations that are short term (weeks) to long term (multi-year) in nature. All services must be provided locally in the San Diego vicinity.

At this time HPE is not able to share additional information about this opportunity. If you would like to be considered for this opportunity please complete the information requested below and use the table to indicate which service(s) your company is able to provide. If you specialize in specific skillsets (i.e. java, .net, etc.) that you would like to highlight, please do so in the notes field located next to the table.

Please provide information only for the services your company is able to provide. If your company is not able to provide a service listed below, please do not enter any information in the table.

If your company is not capable of providing any of the services listed below, please inform HPE of this via email.

The purpose of this ask is to help HPE identify potential vendors for an upcoming opportunity. HPE will follow up with vendors who are able to provide one or more of the services in scope at a later date.

Please understand, a response to this request for information is not a commitment from your company to provide services for Hewlett Packard Enterprise. Hewlett Packard Enterprise does not guarantee business based on your response to this request for information. Responding yes or no to this request will not impact any business you are currently providing to HPE nor will your response impact any active agreements between your company and HPE.

Please complete and return this form via email to Mandi Dundas no later than close of business on **Friday, March 11, 2016.** Should you have any questions, please contact Mandi Dundas via email.

Thank you in advance for your time and participation.

Company Contact Information:

Contact Name:	Click here to enter text.
Company Name:	Click here to enter text.
Address:	Click here to enter text. Click here to enter text.
Phone Number:	Click here to enter text.
Certification ID:	Click here to enter text.

March 2016 HPE Confidential

Services provided by your Company:

Please indicate which of the services below your company is able to provide. If you would like to highlight any skillsets your company specializes in, please capture this information in the notes field. As a reminder, if your company does not provide a skillset listed below please leave the check box blank.

Service Offering:	Service:	Do you provide this service?	Vendor Comments/Notes:
Architects	Apps	☐	Click here to enter text.
	Security	☐	
Project Managers	Agile/Scrum Masters	☐	
Application Development	Mobile Application Development- Xamarin	☐	
	AEM & SharePoint Developers	☐	
Database Administrators	Oracle	☐	
	SQL Server	☐	
SharePoint Administration		☐	
Back-up and Recovery Specialists		☐	
Business Process Analyst/Engineer		☐	

Thank you for your time. Please return completed forms to Mandi Dundas via email no later than close of business on **Friday, March 11, 2016**.

1.5 Volume I Checklist

Print and check the boxes

Proposal Item	Offeror Agrees to Meet?	
Item 1: Offeror's must complete and submit Form P&C 600 FORM (PC-600P) provided as Form in "RFP 7189 IT and Telecommuncation.docx". The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 2: Offeror's must complete and submit the REPRESENTATIONS AND CERTIFICATIONS provided as Form in "RFP 7189 IT and Telecommuncation.docx". The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 3: Offeror's must complete and submit the NONDISCLOSURE INDEMNIFICATION AGREEMENT provided as Form in "RFP 7189 IT and Telecommuncation.docx". The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 4: Offeror's must complete and submit the DVBE REQUIREMENTS AND FORMS provided as Form in "RFP 7189 IT and Telecommuncation.docx". The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 5: Offeror is in agreement and has no exceptions to TERMS AND CONDITIONS. The Offeror must check "Yes" indicating no exceptions, or "No" indicating exceptions are provided	YES ☒	NO ☐
Item 6: Offeror is in agreement and has no exceptions to SCHEDULE A DEFINITIONS. The Offeror must check "Yes" indicating no exceptions, or "No" indicating exceptions are provided	YES ☒	NO ☐
Item 7: Offeror's must complete and submit SCHEDULE 8.1 LICENSE. The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 8: Offeror agrees to meet all the requirements in EXHIBIT JJ-SCHEDULE 19 INSURANCE REQUIREMENT. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 9: Offeror agrees to meet all the requirements in SCHEDULE 12.1.1 INFORMATION PRIVACY AND SECURITY, CRIMINAL OFFENDER RECORD INFORMATION, CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATION SYSTEMS, and COUNTY FACILITY ACCESS. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐

Proposal Item	Offeror Agrees to Meet?	
Item 10: Offeror's must complete and submit - EXHIBIT 12.1.1-1 COUNTY PRIVACY INCIDENT REPORT FORM. The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 11: Offeror's must complete and submit EXHIBIT 12.1.1-2 CORI-CLETS TRAINING REQUEST FORM. The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 12: Offeror's must complete and submit EXHIBIT 12.1.1-3 CLETS EMPLOYEE-VOLUNTEER STATEMENT FORM. The Offeror must check "Yes" indicating compliance, or "No" indicating non- compliance with the requirement.	YES ☒	NO ☐
Item 13: Offeror agrees to meet all the requirements in EXHIBIT 12.1.1-4 CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 14: Offeror agrees to meet all the requirements in EXHIBIT 12.1.1-5 FEDERAL BUREAU OF INVESTIGATIONS CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐

1.6 Offeror Response to Terms and Conditions Questionnaire

1.6.1 Previous, Current, and Future Organizations

Table 1. Previous, Current, and Future Organizations

INFORMATION REQUESTED	RESPONSE
Response	Integrated Property Tax System project
County Agency or Department	Office of the Assessor/Recorder/County Clerk ("ARCC"), the Property Tax Services Division ("PTSD") of the Department of the Auditor and Controller ("A&C")
Description of services performed	Development of a computerized integrated property tax system to provide automated processing of all functions performed by the County relating to the assessment, collection, and disbursement of real property and personal property taxes.
Dates of the engagement (including future end dates)	December 28, 2011 – Present / Estimated Completion February 2017
How these engagements will be affected by this effort	No impact.
The status of the proposal	In progress. Estimated completion by February 2017

1.6.2 Develop/Improve New Service Levels (Schedule 4.8 Service Levels)

HPES is committed to delivering on the Service Levels (SLs) the county requires and will update our measurement methodologies to accommodate the changes in the service levels from the current contract, including posting all SL reports to the Service Portal. This will occur as part of the cross-functional transition that occurs within each framework implementation. During the transition, we will also make the current SL dashboard available from the Service Portal, to authorized County users.

We fully support the SL methodology described in the RFP, and will work with the County to continuously improve SLs so that we are always aware of the performance measures that add the greatest business value. As the county's business requirements evolve to meet the demands of their citizens, HPES will collaboratively add, delete, or change SLs on a yearly basis or at the County's request.

HPES will measure and report our performance against the SLs during each month by the fifteenth (15th) day (or following business day if the fifteenth [15th] is a weekend or holiday) of the following month. In the event that we have failures, we will report these in the months that they occur and in following months, if the failures continue.

In pursuit of continuous improvement, we will review the SLs established with the County one to two times per year and mutually agree on any necessary changes to the performance targets and weightings, to

make sure the service levels continue to be relevant and of value to the County's business. As we implement new initiatives and technology that make higher service levels possible, or offer a better way to manage or measure SL performance, we will recommend these improvements to the County. If increases to target performance levels require additional investment, we will assist the County with assessing the cost/benefit of the incremental increase so that the County may determine if the improvement is in its best interest.

As we implement new services or enhance existing ones, we will discuss new SLs with the County, establish baseline metrics and an improvement plan. Conversely, when SLs are deemed no longer useful to the County, we will retire the processes to measure and manage them, and work with the County to redistribute the service level weights.

1.6.3 Schedule 12.1.1 County's Privacy and Security Requirements

1. Protected Health Information (PHI), as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and

To provide the highest level of information assurance to the County of San Diego, HPES will adhere to the National Institute of Science and Technology (NIST) 800 series special publications for Information Security, which will provide the overall framework and policy guidance to us for the County's security solution. In terms of providing the proper security for the protected health information as defined under the HIPAA law, HPES will utilize the following specific NIST Special Publications – NISTIR-7497 Security Architecture Design Process for HIPAA, and implementing the NIST 800-66 HIPAA Security Rule Toolkit on those systems and platforms that interact with, contain, or manage any data that is classified by the County as containing PHI sensitive information. Additional NIST documentation will be utilized as needed and as it is developed. This approach will ensure compliance to the three main areas within the HIPAA law – Administrative Simplification, Security, and Privacy.

2. Personal Information (PI) as defined under the California Civil Code Section 1798.3. PI may include data provided to the County by the State of California or by the Social Security Administration (SSA); and

3. Personally Identifiable Information (PII) as defined under the Information Exchange Agreement (IEA) between the State of California and the SSA dated _____, which incorporates the Computer Matching and Privacy Protection Agreement (CMPPA) between the SSA and the State of California's Health and Human Services Agency dated _____; and

To further validate that the County has protected all personal information, as defined by California Civil Code 1798.3, and all other data that can potentially cause harm, HPES will continue with the NIST-based Risk Management Framework (RMF) as defined in NIST 800-53 Rev.4 as well as other relevant guidance from the County, State and Federal departments where it applies. HPES will also work directly with the CISO for the County and the appropriate County departments to support each Information Exchange Agreement that exists between the County, the State of California, and the Social Security Administration. HPES will provide ongoing process, architecture, and technical support as needed to make sure that any system changes, upgrades, or new vulnerabilities are mitigated within the County systems that utilize the State and Federal exchanges.

4. Criminal Offender Record Information (CORI) as defined by California Penal Code sections 11075 and 13102, including information from the California Law Enforcement Telecommunications System

(CLETS), the County of San Diego Probation Case Management System (PCMS), and local County records.

The RMF security approach will extend also to Criminal Offender Record Information (CORI) that is contained in the CLETS and PCMS systems as they exist within the County. All relevant records that fall under CORI definition as well as local County records will be protected at the appropriate level with the implication that any unintentional release of data would cause significant harm to the citizens, County, and State.

5. This Schedule does not reduce any other obligation set forth in the Agreement or any other law or regulation governing the information. To the extent another provision of the Agreement requires different protection of information subject to the requirements of this Schedule, the provisions requiring greater protection of the information shall prevail.

1.6.4 HPES Negotiation Team

Table 2. HPES Negotiation Team

NEGOTIATION TEAM MEMBER	TITLE
Steve Tolbert	HPES VP State, Local, and Education (SLED)
Cathy Varner	HPES Account Executive
Mark Searle	HPES Area Sales Leader State, Local, and Education
Grant Book	HPES Senior Counsel
Max Pinna	HPES Contracts Manager
Amer Syed	HPES Client Solutions Executive
Ted Carter	HPES Pricing Lead
Sheelagh Sacks	HPES Solution Lead

1.6.5 Third-Party Applications – Retained Assets

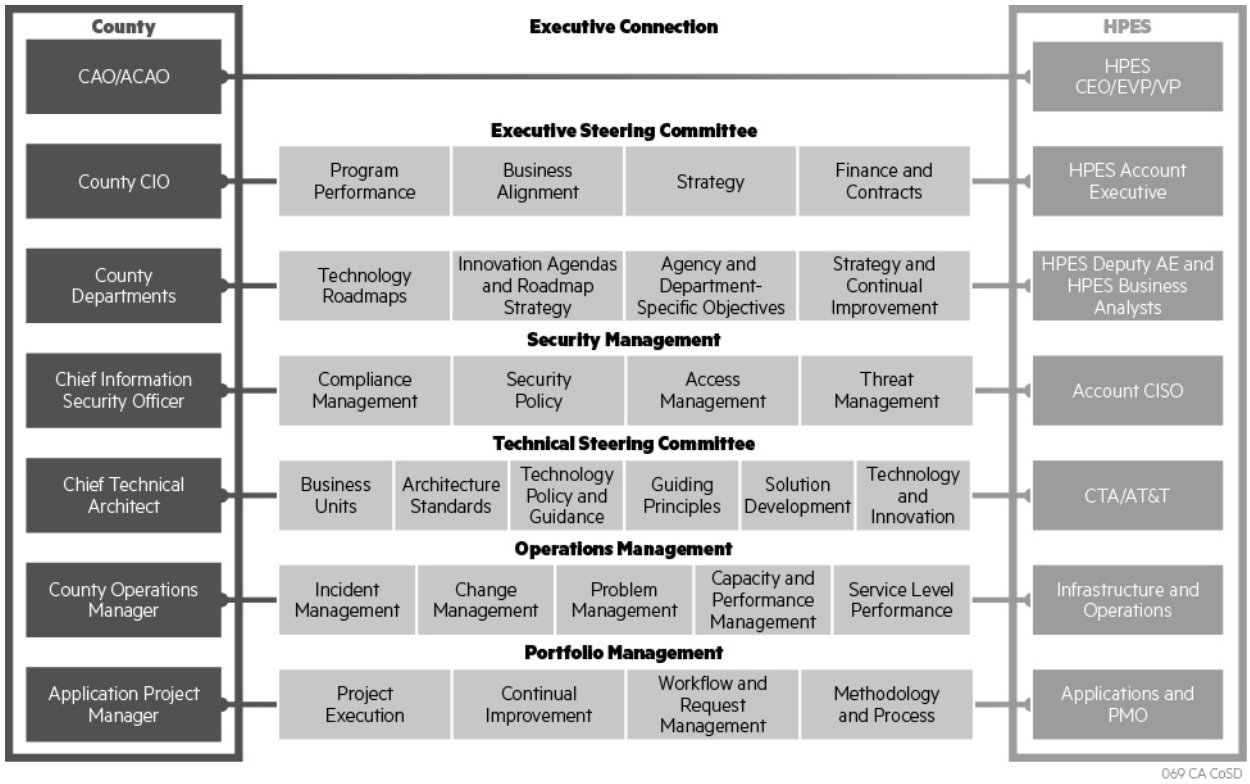
Under the Applications M&O Services, the County defined 169 cloud-based applications that are included as an M&O bundle. HPES will create Service Desk scripts as required for Tier 1 support. The application information will be entered and maintained in the application's CMDB.

Cloud-based retained assets can be submitted for transfer to HPES as third-party software using the existing County and HPES Contract Transfer Request Form. Cloud-based retained assets transferred as third-party software may incur Third-Party Agreement fees.

1.6.6 Relationship Management

HPES has implemented a multitiered relationship framework for communication and decision-making that provides effective collaboration and timely action. This framework, illustrated in Figure 1, maximizes communication based on the County's organizational structure. HPES and County leaders are aligned to the framework to produce results consistent with technical and process architectures. From requirements definition to solution realization, this framework fosters an in depth understanding of business needs and effectively identifies opportunities for innovation and process improvement to the benefit of the County. The framework supports the collaborative development of plans of action based on agreed decisions to achieve the best outcomes for County staff and its citizens. HPES will work with the County to facilitate alignment to the existing governance within the County Technology Office (CTO) and individual County groups.

Figure 1. HPES-County Account Organization Structure



HPES' relationship framework aligns HPES and County leaders to foster clear communication, a solid understanding of business needs, and opportunities for innovation and improvement.

We designed the HPES-County Account organization structure to achieve the best balance of economy and effectiveness. Senior staff are assigned to lead each functional area for this program. The HPES account team is made up of highly qualified experts—with more than 320 years of combined experience supporting the County. This multitiered relationship framework builds mutual trust and results in effective, collaborative interactions, with everyone focused on getting from idea to value as quickly and efficiently as possible.

1.6.6.1 Corporate Changes

We will follow the same communication process we used to notify the County of HP's company split. Initially, the HPES AE spoke to the County CIO and notified him with all available information. Our

CEO sent an email to the County, and other clients. The County is well known to our senior leadership team, and our CEO placed a phone call to the CAO, to personally commit to continued service delivery excellence and to state that the split in no way placed any additional risk on our partnership. Steve Tolbert, VP SLED, also discussed this with the CIO during his regularly scheduled bimonthly meeting. The HPES deputy AE then communicated with the CTO and the Group IT Managers (GITMs) (along with the BAs/APMs) so that the business units heard it directly.

Our AE also contacted AT&T to provide a briefing and answer any questions or concerns, with no changes or disruption.

1.6.6.2 Managing the Overall County Program

Clear lines of communication between the Offeror's team and the County for timely problem identification, mitigation and resolution.

Success of complex IT projects are not just based on IT acumen—successful relationship management and stakeholder communication are critical variables that drive program success. As outlined in Section 2.15 Offeror Response to Exhibit R-Schedule 10.3, HPES has proposed a robust framework for relationship management for the program. Key counterparts have been identified between the County and the HPES program team to make sure the right individuals are aligned across key functions and areas of the program.

To further support that communications are timely, effective, and efficient among the right individuals on the program, a stakeholder communication matrix has been proposed in Section 2.15. The stakeholder communication matrix has been established based on the County's organizational structure to substantiate that County and HPES senior leadership and operational teams are focused and informed on the needs of the County and to facilitate strong communication and collaboration to advance County business and technical objectives. See Table 4.

Interaction with Customer PMs

Governed by the HPES Program Management Office, HPES project managers will interact with the County in a number of ways to communicate program and project status including:

- Regular standing meetings with County stakeholders including County project sponsors, GITMs, and the CTO to discuss project activities including schedule, scope, risks, issues, and/or any concerns requiring escalation.
- Provide program reporting as required or requested by the County regarding the project.
- Conduct frequent reviews of the program risk log to proactively address perceived project risks and associated mitigations to those risks.
- Coordinate cross-functional teams and communication strategies with County sponsors around issue management and work to resolve project performance matters to the County's satisfaction.
- Work with appropriate County stakeholders to address any capacity and demand management issues in a proactive manner.
- Partner with program sponsors and vendors to deliver a consistent and predictable customer experience through established program processes and methodologies for management of the program.
- When process gaps and bottlenecks are identified, establish functional teams to improve processes.

Using the aligned HPES-County organizational structure, we will leverage the existing touch points to implement a formal communication structure that engages County stakeholders early and often throughout the life cycle of the project. Some examples of interactions include:

- Establishing communications strategies for the specific needs of the CTO and County business groups
- Developing enterprise communication procedures and templates
- Auditing program and project communications plans
- Creating PMO and project announcements
- Developing and maintaining communication vehicles such as the PMO SharePoint, public folder, and network drive space
- Publication and management of Notices of Decision
- Creating and executing communication plans for PMO initiatives
- Preparing presentation material for internal and external reporting.

Active and continuing participation and involvement of senior corporate executives in ensuring the success of this program.

A major feature of our organizational structure is the direct access of HPES senior corporate leadership to senior County leadership. Mechanisms are in place to facilitate bidirectional communication between the County and HPES across all layers of the program. Our approach addresses communication to stakeholders at all levels—project, portfolio, and enterprise level. Communications can be facilitated via email or meeting; meetings may be face-to-face and/or teleconference and may include virtual room sessions to discuss matters or view presentation materials and documents.

Cathy Varner, the HPES County of San Diego Account Executive, is dedicated to the County and makes sure the program receives the highest level of commitment from HPES. Cathy is authorized to draw from the vast HPES corporate resources, as needed, to support the accomplishment of program goals and objectives.

Cathy is also directly involved in identifying any new or changing requirements that may require contract changes. In this respect Cathy works closely with Contracts Manager (Max Pinna), the account business manager and the account finance team on identifying such changes and/or any new service or technical solution that may be beneficial to the County. Both Cathy and Max are part of the HPES team colocated at the CAC. As part of the overall program management, Cathy is also included in any dispute that requires her attention. To facilitate a prompt and timely resolution, if necessary, such disputes are discussed in her weekly meetings with the County CIO.

Our team mapping aligns with the County structure and increases our ability to work collaboratively and jointly as we broaden our partnership. The relationship management approach and stakeholder communication matrix identified in the table below enables communication at all levels of the program to make certain that the County has a direct point of contact for all frameworks and their components. Additionally, HPES has established rich relationships with the County, individually and collectively, leading to open and transparent communications that enable dialogue and decisions regarding opportunities and issues.

The meetings listed in Table 3. below are currently ongoing meetings held between the County and HPES to communicate program status and updates so that lines of communication are proactive and maintained at all times.

Table 3. Current and Ongoing Meetings between the County and HPES

COUNTY OF SAN DIEGO	HPES
CIO	Vice President and Account Executive (AE)

COUNTY OF SAN DIEGO	HPES
ACIO	Deputy AE
GITMs	Deputy AE, Enterprise Service Delivery Manager, Service Delivery Managers, Applications Development Services Manager, Project Management Office Manager
CTA	CTA
Contracts Manager	Contracts Manager
Chief Information Security Officer	Chief Information Security Officer
Applications Management	Applications Development Services Manager
Chief Data Architect	CTA
Enterprise Application Project Manager	Project Management Office Manager
Operations Managers	Service Delivery Managers

To enhance this multitiered framework, a complementary communication matrix has been established based on the County's organizational structure and requirements. This matrix substantiates that the County and HPES' leadership and operational teams are focused and informed on the needs of the County. Table 4 outlines the proposed stakeholder communication matrix to facilitate a strong communication and collaboration to advance County business and technical objectives.

Table 4. Proposed Stakeholder Communications

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
Executive Meeting	HPES/County alignment of objectives and program escalations	Bimonthly, or as determined by the County participant	County CIO, HPES VP, SLED, and HPES AE
Program Status and Strategy	Program management overall program health	Weekly	County CIO, HPES AE
CIO Security Briefing	Briefing to County CIO on security strategy, initiatives, and status	Monthly	County CISO. HPES CISO and HPES security officer

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
Executive Liaison Program Meetings	One-on-one communication between HPES AE and key County stakeholders to discuss vision and strategy. Intent is to make certain HPES is prepared to respond to County requirements.	Quarterly, biannually, or annually, as determined by the County participant	County GMs, ROV, DHR, County Council, and select elected officials, HPES AE and/or deputy AE
CTO Enterprise Architecture Meetings	Review enterprise architecture solution designs, annual updates to hardware and software standards for servers, and end-user compute devices, exceptions to standards via notice of decisions, vendor technology roadmaps	Weekly	County CTA, CTO IT Staff, GITMs, County agency and/or department representation, HPES CTA, HPES technology office and other HPES leaders, as needed
Enterprise Architecture Review	Reviews proposed architectural changes, large project designs, architectural issues	Weekly	County CTA, CTO IT staff, GITMs. HPES CTA, HPES technology office, and other HPES leaders, as needed
Network Architecture Meetings	Review network roadmaps and technology upgrades	Weekly	County CTA and other CTO IT staff, HPES CTA, and other HPES technical leaders, as needed, AT&T chief architect
Core Meeting	Preview enterprise solution designs (detailed walkthrough) and changes to standards	Weekly	County CTA, CTO IT staff and CISO, HPES CTA, HPES CISO, and other HPES leaders, as needed
Infrastructure Project Review	Provides schedule, issue, and status data for active infrastructure projects	Weekly	County CTA, GITMs, CTO IT staff, HPES CTA, HPES technology office, and other HPES leaders, as needed
Platform Status Reviews	Review project for critical County application platforms	Weekly	County CTA, CTO IT staff, HPES application development

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
			leader and other HPES leaders, as needed
Portfolio Review	Provide review of high visibility, critical projects	Monthly	County CTA, GITMs, and CTO IT Staff. HPES business analysts, HPES deputy AE and other HPES leaders, as needed
Portfolio Steering Committees	Review portfolio and future plans	Quarterly	County GITMs, HPES business analysts, and other HPES leaders, as needed
ITPMO Review	Discuss processes and procedures related to project management and process improvement with CTO	Weekly	County CTO IT staff, CTA, HPES PMO and other HPES leaders, as needed
Quarterly Program Review	Provide program status, accomplishments, and operational data	Quarterly	County CTO IT staff, CTA and GITMs, HPES AE, deputy AE, and other HPES leaders, as needed
Service Delivery Operations	Mitigation/review of operation changes and issues with CTO	Biweekly	County CTO IT staff, CTA, HPES service delivery executive, and other HPES leaders, as needed
Service Delivery Operations Monthly	Mitigation/review of operation changes and issues with the CTO and GITMs	Monthly	County CTA, CTO IT staff, and GITMs, HPES service delivery executive, SDMs, and other HPES leaders, as needed
County Bricks (Technology Standards)	Document past, current, and future technology standards using Gartner's brick framework. Bricks guide solutions for the County and is updated when there are specific changes to a technology item.	As needed, triggered by product, vendor, or technology changes	County CTO IT staff, CTA, GITMs, HPES CTA, HPES technology office and other HPES leaders, as needed

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
Voice of the Client (VOC) – Service Excellence Initiative	Includes self-assessed ratings pertaining to delivery and client satisfaction results based on client survey feedback; our objective is continual improvement of client satisfaction and retention	Yearly	County CTO IT staff, HPES VOC interviewer
Information Technology Improvement Needs Assessment (ITINA) Process	HPES provides support for the County enterprise IT project planning and budgeting process—prioritization, estimating, and selection for County enterprise IT initiatives	Yearly	County IT Planning Board, GITMs, CTO IT staff, HPES participants based on subject matter expertise

1.7 Offeror Response to Terms and Conditions Exception List and Redline

1.7.1 Exception List

The exceptions noted in previous proposal submissions are withdrawn based upon the final version of the terms and conditions negotiated by the parties. As such, HPES has no exceptions as part of this proposal submission.

1.8 Offeror Response to "Exhibit P: Schedule 8.1 License for Use of County Facilities and Property"

HPES agrees to complete Exhibit P-Schedule 8.1 for Use of County Facilities and Property at time of award.

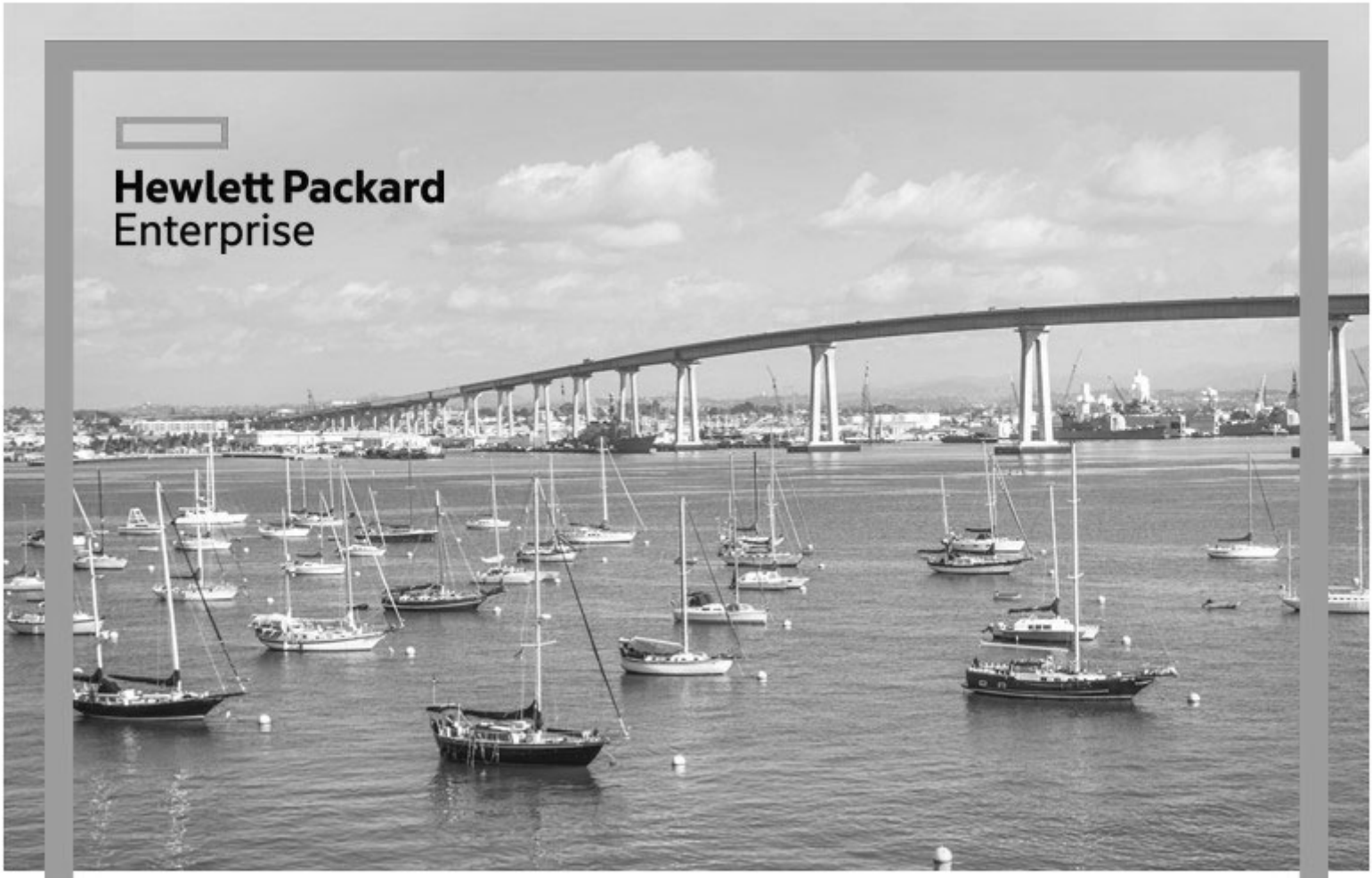
1.9 Appendix

Exhibit A: Terms and Conditions

RFP 7189 Exhibit A:

Terms & Conditions

The exceptions/redlines noted in previous proposal submissions are withdrawn based upon the final version of the terms and conditions negotiated by the parties. As such, HPES has no exceptions as part of this proposal submission.



Hewlett Packard
Enterprise

Driving Results

Committed, progressive partner moving the County forward through innovation and continuous improvement

HP Enterprise Services' Response to the County of San Diego Request for Proposals (RFP) 7189 – Information Technology & Telecommunications Services

Final Submission

October 2016

Volume II - Technical Proposal

Executive Summary

In recent years, the County of San Diego has transformed the way residents and visitors receive valuable services, obtain information and interact with County officials. With successful efforts to provide digital government, mobility services, business continuity and workforce optimization, the County has been recognized as one of the nation's most technologically advanced counties, achieving numerous awards and accolades. Whereas recognition is notable, the beneficial impact to County employees, taxpayers and residents is what is truly impressive. HPES is proud to have been your partner over the past 10 years in this drive to achieve operational excellence.

HPES understands the County's mission to improve the lives of San Diegans through Safe Communities, Sustainable Environments, Healthy Families, and Operational Excellence. The technology foundation enabling the support of these initiatives relies on systems and services delivered and maintained by our team. Our approach and performance provides the County peace of mind that IT is being managed properly so you can focus on that noblest of motives, the public good.

We must also continue to address the challenges facing County residents, particularly those in danger of being disenfranchised, Veterans, foster children, the homeless, and those suffering from mental illness. We view our role in the County, not just in the context of technology, but as a key enabler to better business outcomes as you strive to "connect the unconnected."

San Diego County has a proud military heritage. Our team will implement programs to support military residents and returning Veterans. Working with groups such as Mission Edge San Diego (Three Wise Men), we will develop training programs tailored for military personnel with the goal of providing the technology skills required to be competitive in the job market.

The County has been successful in raising the "IT IQ" of County personnel. We embrace this concept and will, in collaboration with CTO and support from key providers like Adobe and Microsoft, deliver training programs for County personnel focused on transformative learning that will enable them to most effectively utilize the capabilities and functionality of software and services in which the County is investing.

Our approach to providing IT services to the County has always been to deliver the right solution at the best price, in line with County's strategic objectives. Our commitment is to build on that approach. We have strong relationships with top tier providers including EMC, Oracle and IBM. Whether a technology comes from a strategic partner or a perceived competitor, we will bring the best solution to the County to achieve the best business outcome. The delivery of reliable, predictable and quality results, with high end-user satisfaction, is of utmost importance to us. We are pleased to note that together with County CTO, we achieved the highest rating to date in the annual Gartner IT customer satisfaction survey, reaching the top category, "Best in Class".

Operational excellence requires the pursuit of continuous improvement. At all levels across our organization, our focus on problem solving, teamwork and leadership will ensure we consistently identify and seize opportunities to provide optimal results. The transformative specifics in our proposal provide mechanisms the County can leverage to foster new ways of thinking and spark creativity among our teams across the County, industry partners, and constituents. We will ensure a sound foundation from which the County can address current challenges as well as provide services to the next generation resident - one who is proactive, connected, and aspiring to contribute. Like the County, we believe that "Good Government Demands the Intelligent Interest of Every Citizen" and we will collaborate with the

County to identify and implement technologies and programs to encourage that interest, and enable every citizen to be engaged.

Building on the vision established by the CTO, HPES developed a local Innovation Council. The council's charter is to address real business needs, increase efficiency and reduce County spend. Once a year, we host Innovation Day at the COC for all interested County users where these innovation ideas are showcased. Since 2014, the Innovation Council has presented 26 ideas, 10 of which have been implemented into production. These solutions have had a positive impact on County users and citizen-centric services.

HPES is honored to be a Live Well San Diego partner. Our commitment to the community is also demonstrated through engagements like election night support, fielding a team for the Live Well San Diego 5K, sponsoring and attending the State of the County address, and providing speakers and technical support for County events such as Passport to Life Career & Education Expo and the Dick Wayman Technology Center Ribbon Cutting Ceremony at the Ramona Library. At numerous other County events you will find the employees of HPES and our partner AT&T in the mix; participating, supporting and occasionally sponsoring. We are engaged and involved on a personal level.

And for good reason: We live here. Our highly qualified team is primarily comprised of San Diego County residents. We understand what we do matters, to our families, our friends, our neighbors, and the entire San Diego region.

You will see many familiar names in our list of 20 Key Personnel; individuals who have worked shoulder to shoulder with the County delivering consistent results, solving problems and building a relationship of trust. The team will continue to be led by Cathy Varner, our current and proposed Account Executive, who has been supporting the County since 2006. Our telecommunications partner, AT&T, will continue to be led by Grant Morgan, who has also supported the County for 10 years. Together, our team has a broad set of skills uniquely suited to supporting the County. From architects and engineers to service desk and desk side support, we are steadfast in our commitment. We are knowledgeable of County business and culture and we demonstrate that knowledge in every aspect of our performance.

It has been a privilege for HPES to support the County's IT and Telecommunications for the past 10 years. We do not take for granted the trust the County has placed in us. Our core tenet has been and will continue to be, "we must earn the opportunity to do business with the County". As the incumbent, our knowledge and experience presents the lowest risk transition. We will continue to consistently deliver the County's IT operations while we transition and transform to the technologies required by the new scope of work and beyond.

The new frontier for our partnership will be a model of excellence in reliability, continuous improvement, transformation, and strategic alignment, advancing the gauge for County staff, constituents, and visitors.

As we move forward in our partnership, you can be assured that your reputation as the best managed local government in America will continue to be affirmed.

Table of Contents

Executive Summary ..... **i**
2. Technical **1**
2.1 Volume Checklist 2
2.2 Offeror Response to Qualifications and Experience Questionnaire 4
2.2.1 Number of Years as Prime Contractor 4
2.2.2 Customer References 5
2.3 Offeror Response to Organization and Staffing Questionnaire 29
2.3.1 Overall Organization Chart 30
2.3.2 Proposed Staffing Organization Chart 30
2.3.3 Centers of Excellence 31
2.3.4 Proposed Key Personnel 32
2.3.5 Project Staff Selection and Replacement 45
2.4 Service Framework Executive Overview 48
2.5 Cross-Functional Services Framework 49
2.5.1 Contract and Acquisition Management (Sched 4.3, Section 2.3) 51
2.5.2 Integrated Asset Management Services (Sched 4.3, Section 2.4) 54
2.5.3 Billing Management (Sched 4.3, Section 2.5) 64
2.5.4 Security Management (Sched 4.3, Section 2.6) 67
2.5.5 Service Delivery Management (Sched 4.3, Section 2.7) 81
2.5.6 (Reserved) 87
2.5.7 Project Management (Sched 4.3, Section 2.9) 87
Integration and Testing Services (Sched 4.3, Section 2.10) 95
2.5.8 Incident Management (Sched 4.3, Section 2.11) 104
2.5.9 Problem Management Services (Sched 4.3, Section 2.12) 110
2.5.10 Change Management Services (Sched 4.3, Section 2.13) 115
Release Management Services (Sched 4.3, Section 2.14) 119
2.5.11 Configuration Management Services (Sched 4.3, Section 2.15) 122
2.5.12 Capacity Planning and Performance Management Services (Sched 4.3, Section 2.16) 126
Disaster Recovery Management Services (Sched 4.3, Section 2.17) 131
2.5.13 Identity and Access Management Services (Sched 4.3, Section 2.18) 137
Reporting Management Services (Sched 4.3, Section 2.19) 144
Domain Name Management Services (Sched 4.3, Section 2.20) 147
2.5.14 Business Analyst Services (Sched 4.3, Section 2.21 149
Chief Technical Architect (Sched 4.3, Section 2.22) 161
Enterprise Application Architect (Schedule 4.3, Section 2.23) 171
Innovation Management Services (Sched 4.3, Section 2.24) 173
2.5.15 Executive Summary 175
2.6 Service Desk Services Framework 190
2.6.1 Service Desk Services Specific Questions 199

2.7 End-User Services Framework 214
2.7.1 Offeror Response to End User Services Specific Questions 254
2.8 Network Services Framework 272
2.8.1 Offeror Response to Network Services Specific Questions 330
2.9 Data Center Services Framework 355
2.9.1 Offeror Response to Data Center Services Specific Questions 429
2.10 Applications Services Framework 443
2.10.1 Offeror Response to Application Services Specific Questions 464
2.11 Transition Services 486
2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5) 496
2.12 Transformation Services 559
2.12.1 Transformation Services (Exhibit KK, Section 2.4, 2.5, 2.6) 560
2.13 Offeror Response to Exhibit O-Schedule 7.6 Shared Resources 630
2.14 Offeror Response to Exhibit Q-Schedule 10.1.1 Contractor Key Personnel 638
2.15 Offeror Response to Exhibit R-Schedule 10.3 Relationship Management 639
2.15.1 Relationship Counterpart 640
2.16 Offeror Response to Exhibit Y: Schedule 14.1 Approved Subcontractors 643
2.17 Assumptions 644
2.18 Offeror Response to Technical Exception List 645
2.19 Appendix - Completed Exhibits 647
Exhibit O: Schedule 7.6 Shared Resources 648
Exhibit Q: Schedule 10.1.1 Contractor Key Personnel 656
Exhibit R: Schedule 10.3 Relationship Management 657
Exhibit Y: Schedule 14.1 Approved Subcontractors 661

2. Technical

2.1 Volume Checklist

2. Technical

The Technical Section, including all schedules, exhibits, and questionnaires thereto. The Technical evaluation will include the areas listed below.

Proposal Item	Offeror Agrees to Meet?	
Item 1: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – OVERVIEW OF SERVICES. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 2: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – CROSS FUNCTIONAL SERVICES FRAMEWORK. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 3: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – SERVICE DESK SERVICES FRAMEWORK. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 4: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – END-USER SERVICES FRAMEWORK. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 5: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – NETWORK SERVICES FRAMEWORK. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 6: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – DATA CENTER SERVICES FRAMEWORK. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 7: Offeror agrees to meet all the requirements in SCHEDULE 4.3 – APPLICATION SERVICES FRAMEWROK. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 8: Offeror agrees to meet all the requirements in SCHEDULE 4.4 – ASSET MANAGEMENT UPGRADES AND ENHANCEMENTS. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 9: Offeror agrees to meet all the requirements in SCHEDULE 4.8 – SERVICE LEVELS. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☐	NO ☒
Item 10: Offeror agrees to meet all the requirements in SCHEDULE 4.8-1 – SPECIAL SERVICE LEVEL REQUIREMENT. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 11: Offeror agrees to meet all the requirements in SCHEDULE 5 – INVOICES AND REPORTS. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 12: Offeror agrees to meet all the requirements in SCHEDULE 7.2 END-USER SATISFACTOIN SURVEYS. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐

Proposal Item	Offeror Agrees to Meet?	
Item 13: Offeror agrees to meet all the requirements in SCHEDULE 7.3.1 STANDARDS AND PROCEDURES MANUAL. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 14: Offeror's must complete and submit SCHEDULE 7.6 SHARED RESOURCES. The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 15: Offeror agrees to meet all the requirements in SCHEDULE 10.1.1 CONTRACTOR KEY PERSONNEL. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 16: Offeror's must complete and submit SCHEDULE 10.3 – RELATIONSHIP MANAGEMENT. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements	YES ☒	NO ☐
Item 17: Offeror's must complete and submit SCHEDULE 14.1 APPROVED SUBCONTRACTORS. The Offeror must check "Yes" indicating compliance, or "No" indicating non-compliance with the requirement.	YES ☒	NO ☐
Item 18: Offeror agrees to meet all the requirements in SCHEDULE 2.1 TRANSITION PLAN. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 19: Offeror agrees to meet all the requirements in EXHIBIT KK TRANSFORMATION REQUIREMENTS. The Offeror must check "Yes" indicating agreement, or "No" indicating non- agreement with the requirements.	YES ☒	NO ☐

2.2 Offeror Response to Qualifications and Experience Questionnaire

2.2.1 Number of Years as Prime Contractor

2.2.1. Indicate the number of years your organization has acted as a Prime Contractor (and the number of years of experience, if different) providing IT and telecommunications services similar to those described in this RFP specifically to governmental agencies at the United States federal, state or local level (including the District of Columbia).

With a California legacy that dates back to a partnership founded in 1939 by William R. Hewlett and David Packard, Hewlett Packard Enterprise (HPE) strives every day to uphold and enhance that legacy through our dedication to providing innovative technological solutions to our customers, such as the County of San Diego.

In 2008, Hewlett-Packard Company reached a deal with EDS to acquire the company. One year later EDS became HP Enterprise Services, LLC (HPES), which forms the core of Hewlett Packard Enterprise.

Since 1962, and 54 years later, Hewlett Packard Enterprise has been a prime contractor providing IT and telecommunications services. EDS was a pioneer in facilities management (becoming the IT department for many customers, which is now called Information Technology Outsourcing [ITO]) as well as beginning to service and provide early support for Medicaid and Medicare in its home state of Texas. With a long history of serving the public sector, Hewlett Packard Enterprise understands the unique requirements of state and local government, Federal, healthcare, and education customers in the United States. The County of San Diego is recognized throughout the United States as one of the largest and most successful examples of how an ITO delivery model should work. State and local, Federal, U.S. Department of Defense (DoD), intelligence, and education segments, as well as global companies, know about the County, its services, recognition, and accolades.

It takes a reliable and knowledgeable team to deliver ITO services. We take pride in building a solid working relationship with AT&T and the many vendors that we manage; we hold them to the high standards the County expects.

The state and local segment strives to improve the efficiency and effectiveness of state, county and city governments across the country; today we have 34 state and local contracts. In addition, we provide large-scale IT and telecommunications contracts to the following:

- County of San Diego – Since 2006 we have been providing enterprise-wide infrastructure management support services to the County, and in 2011 we became the prime contractor, supporting 16,000 users and 40 departments.
- The Navy Marine Corps Intranet (NMCI) // Next Generation Enterprise Network (NGEN) – Since 2001 we have been managing and securing the world's largest private network for the U.S. Department of the Navy, serving 800,000 users at 2,000 global locations.
- City of Anaheim – Since 2003 we have been providing 24x7 enterprise IT services to support 1,500 staff members at multiple city locations.
- California Department of Corrections and Rehabilitation (CDCR) Strategic Offender Management System (SOMS) – Our team implemented electronic SOMS—providing an integrated, centralized case management tool to help gain operational efficiencies, improve safety for staff and the general public, and increase enterprise visibility into agency information; SOMS enabled the retirement of more than 40 legacy systems.
- The Department of Housing and Urban Development (HUD) Information Technology Service – We provide enterprise-wide IT infrastructure and data center services; Disaster Recovery (DR) services; and support for more than 200 applications running on mainframe, midrange, client/server, and PC platforms.

- U.S. Centers for Medicare & Medicaid Services Enterprise Data Center – Our technical solution and additional DR options continue to provide increased levels of service and economies of scale that are unprecedented in the Virtual Data Center (VDC) community of data centers.
- VDC – Our team supports more than 8 million users, 35 application business owners, more than 4,000 servers, more than 500 network and security devices, and multiple storage platforms at three managed data centers and at AWS.
- Defense Information Systems Agency (DISA) – We provide on-demand processing, capacity, storage, software, content delivery services, and professional services as a managed service for DISA's Computing Services Directorate through the Server Processor Environment (SPE) contract to bring scalable, on-demand processing capabilities to DISA's 17 computing service data centers and future locations approved by the Agency.

2.2.2 Customer References

Table 1 lists five customer references from HPES (proposed prime contractor) and an additional five customer references from AT&T (proposed subcontractor). To be concise Table 1 lists 10 public sector U.S.-based customers for whom we and AT&T provide services that align favorably with at least two or more of the County's five Service Frameworks. Toward the back of this section we provide additional Category of Service detail for each of our five HPES references.

Table 1. HPES and AT&T references mapped to the County's five Service Frameworks.

#	NAME OF REFERENCE CLIENT	SERVICE FRAMEWORKS PROVIDED				
		1 Service Desk	2 End User	3 Network	4 Data Center	5 Application Services
References from HPES (proposed prime contractor)						
1	County of San Diego	✓	✓	✓	✓	✓
2	U.S. Department of Housing and Urban Development	✓	✓	✓	✓	✓
3	Department of the Navy	✓	✓	✓	✓	✓
4	California Department of Corrections and Rehabilitation	✓		✓	✓	✓
5	City of Anaheim	✓	✓	✓	✓	✓
References from AT&T (proposed subcontractor)						
1	County of San Diego	✓	✓	✓		
2	State of Georgia	✓		✓		
3	State of Tennessee			✓		
4	State of Michigan	✓		✓		
5	State of California	✓		✓		

HPES CONTRACT 1 – COUNTY OF SAN DIEGO

Customer Reference Number	1 of 5 HPES contract references
Client Name	County of San Diego
Contract Title/Contract Reference Number	IT and Telecommunications Services Agreement Contract No. 0040007225
Primary Contact, Title and Telephone Number	Dorothy R. Gardner, IT Contract Manager, (619) 531-5361
Contract Dates	May 2011 – January 2018 (prime) January 2006 – April 2011 (sub to NG)
Contract Amount	Approximately $120 million per year
Type of Contract (Public/Private Sector)	Type: Firm Fixed Price, T&M with Volume Metrics Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (2) End-User Services (3) Network Services (4) Data Center Services (5) Application Services.
Length of Relationship with Client	10+ years

Description

HPES performs all Information Technology Service Management (ITSM) for the County, including help desk, data center, end-user computing, printers, hardware and software asset management, end-user computing device engineering, configuration management, change management, IT procurement, IT subcontracting, mainframe, servers, storage, network, applications support, application development, infrastructure and application architecture, and security.

HPES CONTRACT 2 – U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT (HUD)

Customer Reference Number	2 of 5 HPES contract references
Client Name	U.S. Department of Housing and Urban Development (HUD)
Contract Title/Contract Reference Number	HUD Information Technology Services (HITS) and follow-on HITS-Continuity of Services (CS) HITS Contract No. C-OPC-22807 HITS-CS Contract No. DU100F-15-C-05
Primary Contact, Title and Telephone Number	Kelly Wong, Program Manager, Office of Chief Information Officer, (202) 402-8036
Contract Dates	HITS Contract: February 2005 – October 2014; HITS-CS contract: November 2014 – July 2017
Contract Amount	$619 million

HPES CONTRACT 2 – U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT (HUD)

Type of Contract (Public/Private Sector)	Type: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (2) End-User Services (for mobile users) (3) Network Services (4) Data Center Services (5) Application Services.
Length of Relationship with Client	11 years

Description

Implementing a roadmap for change that we helped develop, HPES took HUD from inflexibility and lack of integration to integrated, standards-based services for approximately 80 sites nationwide, across 50 U.S. states and 16 U.S. territories. HUD now has a very Agile, responsive, highly available, and scalable IT environment that runs its legacy applications and allows HUD's next-generation web applications to "go live" on time and successfully. Our HUD HITS program is certified at International Organization for Standardization (ISO) 20000 quality standards and is firmly founded on Information Technology Infrastructure Library (ITIL)-based processes. We have conducted more than 10 technical innovation forums to introduce new technologies or concepts for HUD's consideration.

FISMA and PMA Achievements

With our support, HUD raised its Federal Information Security Management (FISMA) rating from F to A+ within 2 years of the start of the HITS contract.

Because of our critical contributions, HUD achieved a coveted milestone: a "green" rating from the Policy Management Authority (PMA).

Our 20 HITS contract Service Level Agreements (SLAs) are as follows: hardware support, software support, database management, enterprise engineering, telecommunications, wireless and mobile communications, performance modeling, technology assessment, help desk, system acceptance, Disaster Recovery (DR), integration and test, electronic data interchange (EDI), facilities management, security, configuration management, program management, HITS data center LAN/WAN administration, storage management, and end-user support.

HPES CONTRACT 3 – U.S. DEPARTMENT OF THE NAVY

Customer Reference Number	3 of 5 HPES contract references
Client Name	Department of the Navy (DON), U.S. Navy Marine Corps, Space and Naval Warfare Systems Command
Contract Title/Contract Reference Number	Navy Marine Corps Intranet (NMCI), Continuation of Services Contract, & Next Generation Enterprise Network (NGEN) NMCI Contract Number: N0002400D6000 CoSC Contract Number: N00039-10-D-0010 NGEN Contract Number: N0003913D0013
Primary Contact, Title and Telephone Number	Kim Reavis, Contracting Officer, (703) 595-3363

HPES CONTRACT 3 – U.S. DEPARTMENT OF THE NAVY

Contract Dates	NMCI: October 2000 – September 2010; CoSC: October 2010 – July 2015 NGEN: July 2015 – September 2018
Contract Amount	NMCI: $9.3 billion; CoSC: $3.4 billion; NGEN $3.5 billion
Type of Contract (Public/Private Sector)	Contract Type: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (2) End-User Services (4) Data Center Services (5) Network Services (6) Application Services.
Length of Relationship with Client	15 years

Description

The U.S. Department of the Navy (DoN) operates one of the largest intranets in the world, Navy Marine Corps Intranet (NMCI). NMCI provides end-to-end, secure IT services to more than 400,000 seats and 900,000 users, across more than 2,500 locations that vary from major bases to single-user locations. NMCI NGEN requires delivery of 34 IT enterprise services with life-cycle governance, security, availability, and technology refresh capabilities. The 34 services are grouped into cybersecurity, enterprise management, end user, and network services. HPES has provided continuous support for the DoN's NMCI Program since its inception in 2001. The program has spanned three major contracts, all of which were awarded to HPES as the prime contractor.

Under the NGEN contract, HPES and our team members provide comprehensive IT services to the U.S. Navy (USN) and staffing support to the U.S. Marine Corps (USMC). We are implementing IT Service Management (ITSM) processes to provide enhanced Command and Control (C2)—creating new processes, improving existing processes, and transferring process management to the enterprise level.

NGEN is administered as a fixed price contract with costs associated with delivery of services (seats). DoN pays a fixed dollar amount per seat, allowing it to manage predictable budgets. The number of managed hardware assets exceeds 500,000—93,000 of which are related to seats (desktop, monitor, keyboard, and mouse). The remaining hardware assets consist of servers, switches, routers, peripherals, and other catalog items. We also manage more than 2 million software licenses.

NMCI NGEN Quick Look:

- Supports 230,000+ Navy devices, including approximately 22,000 mobile devices
- Delivers VTC services from 525 end points
- Transfers 33 million+ email messages weekly—incorporating 20 TB of data daily
- Handles 664 million browser interactions annually
- Stores 20.6 PB of data daily
- Blocks 35 million spam messages monthly
- Uses ITIL V3 service delivery model aligned with ISO 2000.

Significant Cost Avoidance

Beginning in 2014, we managed the program's first NGEN seat refreshes, refreshing 63,500 existing seats and delivering 17,400 new seats to date.

By accelerating transition to 90 days, we helped the Government achieve a cost avoidance of $20 million per month.

HPES CONTRACT 4 – CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION

Customer Reference Number	4 of 5 HPES references
Client Name	California Department of Corrections and Rehabilitation (CDCR)
Contract Title/Contract Reference Number	Strategic Offender Management System (SOMS) Contract No. CDCR 5225-113
Primary Contact, Title and Telephone Number	Scott Davidson, SOMS Project Director, (916) 358-2201
Contract Dates	Original contract: May 2009 – July 2014. Extension: July 2014 – June 2019
Contract Amount	$41.9 million annual gross revenue
Type of Contract (Public/Private Sector)	Contract Type: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (3) Network Services (4) Data Center Services (6) Application Services
Length of Relationship with Client	6.5 years

Description

The California Department of Corrections and Rehabilitation (CDCR) operates 34 adult institutions, 12 community correctional facilities, 40 camps, and 5 prisoner mother facilities—housing approximately 133,000 adult offenders. In addition, parole agents supervise 114,000 adult parolees and 3,000 juvenile parolees from nearly 100 locations throughout California. The CDCR is responsible for the Strategic Offender Management System (SOMS)—an integrated electronic offender management information system—that is one of the largest IT deployments in corrections in the United States

The SOMS project supports state public policy goals, represents an innovative use of new technology in California, and assists Government officials in executing their duties by enabling data sharing with other law enforcement and judicial agencies, such as the Department of Justice (DOJ) and the Department of State Hospitals.

Positive Reengineering Outcomes

- The implementation of SOMS reengineered and greatly improved many business processes and functions that affect 34 institutions and various administrative locations.
- As a result of these changes, institution staff, inmates, and the public are now safer.
- CDCR is recognizing savings as a result of the reduction of paper generated in manual processes, staffing reductions, and improved business process efficiencies.
- All files are now scanned and available electronically for CDCR access statewide.

SOMS is composed of three primary components: (1) an integrated central offender database, (2) a web-based offender management application, and (3) a comprehensive document management system, the Electronic Records Management System (ERMS). SOMS consolidates existing databases and records; automates manual, paper-based processes; converts paper files to digital files; and provides enterprise-wide access to data. SOMS provides benefits to CDCR

by improving staff and inmate safety with secure access to accurate and complete offender information and by increasing staff efficiency, effectiveness, and accuracy by providing access to real-time information in a single database.

As the prime contractor, HPES manages all aspects of the SOMS project for the CDCR. We provide a full range of IT solutions and applications development services that include program and project management, testing, business intelligence and analytics, database support, imaging, and technical support. Our solution includes the following specific activities and tasks:

Document Digitization Success

- We scanned 10.7 million documents, consisting of multiple pages, into the ERMS back file.
- The average number of pages per document is 28, so roughly 300 million images were scanned.

This stands as one of the largest back-file digitization efforts ever undertaken in the state and local market.

- Architect, install, and operate system hardware and software to support the application development life cycle (i.e., development, testing, training, performance testing, and production support).
- Conduct system testing, performance testing, and integration testing of the solution.
- Provide requirements elaboration and traceability.
- Conduct design sessions to define customizations of the COTS offender management system necessary to meet specific needs of CDCR.
- Develop web-based training and lead customer-facing training sessions.
- Conduct on-site readiness assessments at 33 state prisons in preparation for deploying the solution.
- Provide 24x7 production support.

HPES CONTRACT 5 – CITY OF ANAHEIM, CALIFORNIA

Customer Reference Number	5 of 5 HPES contract references
Client Name	City of Anaheim, California (the City)
Contract Title/Contract Reference Number	Title: Information Technology Services Contract No. 0040004644
Primary Contact, Title and Telephone Number	Trevor Bennett, IT Manager, City of Anaheim, (714) 576-5127
Contract Dates	Original Contract: March 2003 – February 2014 Renewed Contract: March 2014 – February 2019
Contract Amount	$100 million
Type of Contract (Public/Private Sector)	Contract Type: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (2) End-User Services (3) Network Services (4) Data Center Services (5) Application Services.
Length of Relationship with Client	13 years

Description

The City of Anaheim was incorporated in 1857 as a charter city operating under a Council-Manager form of government. The City borders encompass an area in excess of 50 square miles with a population of 351,433 residents. The City of Anaheim does not have a central campus style facility arrangement, but it is dispersed across the City boundaries for better customer care relationships. This disbursed workforce location arrangement provides a challenge for IT that HPES has fully embraced.

HPES provides end-to-end services to enhance Government efficiency, reduce costs, and offer citizens and businesses easy access to Government services online in a secure environment. City entities serviced by the contract include the City's Finance, Payroll, Public Utilities, Fire, and Police departments. We and the City sponsors manage projects collaboratively. Our approach includes on-site HPES delivery leaders who provide the City with a single point of accountability and are empowered to allocate the needed resources to meet the City's changing requirements.

Anytime, Anywhere Access to Critical Information

- Virtual emergency command center
- Interactive, web-based portal
- Open architecture foundation
- Anytime, anywhere access
- Geographic Information System (GIS)-centric
- Live video feeds
- Highly scalable

EVOC helps decision-makers ascertain how many police units are on the scene, how many fire units are on the way, and even what a 911 caller said about a particular incident—all in real-time, using any secure Internet connection.

Services we provide include the following: network, application, Service Desk, mainframe and mid-range computing, desktop computing, break/fix repair, system security, and disaster planning and recovery for approximately:

- 2,400 desktops
- 700 laptops
- 1,500 mobile phones
- 100 tablets
- 4,000 voice stations (approximately 400 of which are on VoIP).

We helped the City of Anaheim build, implement, and operate its Enterprise Virtual Operations Center (EVOC), which brings together critical information from the City's Fire, Police, and other departments into a modern, interactive portal—using an open architecture foundation. Authorized decision-makers have anytime, anywhere access to this virtual solution, which is designed to quickly scale to handle increased volumes of critical information during emergencies. EVOC even allows City officials to tap into blueprints, utility plans, and video cameras throughout the City to obtain a live feed of what is happening on the scene. Implemented in just 6 months, Anaheim's virtual command center makes it possible for City officials to see what is happening on all of the City's critical response fronts with just one click.

AT&T CONTRACT 1 – COUNTY OF SAN DIEGO

Customer Reference Number	1 of 5 AT&T contract references
Client Name	County of San Diego (the County)—as a subcontractor to HPES
Contract Title/Contract Reference Number	IT and Telecommunications Services Agreement Contract No. 0040007225
Primary Contact, Title and Telephone Number	Dorothy R. Gardner, IT Contract Manager,

AT&T CONTRACT 1 – COUNTY OF SAN DIEGO

	(619) 531-5361
Contract Dates	May 2011 – January 2018 (as sub to HPES) January 2006 – April 2011 (as sub to NG)
Contract Amount	Approximately $33 million per year
Type of Contract (Public/Private Sector)	Type: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk (2) End User Services[1] (3) Network Services
Length of Relationship with Client	30+ years

[1] *Applies to VPN solutions and Unified Communications (UC) services.*

Description

As a major subcontractor to—and partner with—HPES on the County's IT Outsourcing contract, AT&T provides all of the voice and data network framework services that support the County-wide WAN.

Service Framework 1 – **Service Desk Services.** AT&T staffs its Tier 2 Help Desk daily from 6:00 a.m. to 6:00 p.m., PT. From that desk, AT&T handles network, data, and end-user services, including equipment used to provide the network framework services as stipulated in the contract. AT&T handles priority tickets after hours; otherwise those tickets revert to help desk assistance the next day. AT&T monitors and tracks customer service closely on such tickets, which have strict penalties for missed contract service levels. To support the County's increasing use of technology, AT&T expanded its help desk levels of support in areas such as mobility and remote access.

Service Framework 2 – **End User Services.** AT&T provides Virtual Private Network (VPN) solutions for mobile users using NetMotion with SSL VPN application persistence in the data centers and PulseSecure VPN. AT&T also provides a completely managed Citrix stack to optimize end-user access to all applications through the network. Other end-user services that AT&T provides include a custom-hosted Avaya PBX for Unified Communications (UC) services; VoIP, Business Voice over IP (BVoIP); and voice messaging with text-to-voice functionality, softphones, and Instant Messaging and Presence using Office 365 in a hybrid environment.

Service Framework 3 – **Network Services.** AT&T provides voice and data infrastructure and transport to all County sites. These network services include monitoring, maintenance, help desk, Internet access, and security—all of which AT&T manages in a proactive way that adheres to strict SLA requirements. Cloud-based services that AT&T provides include AirWatch Mobile Device Management (MDM), external DNS via Akamai, speech-to-text voicemail translation using Mutare, and Digital Loss Prevention (DLP) services using Websence.

AT&T CONTRACT 2 – STATE OF GEORGIA

Customer Reference Number	2 of 5 AT&T contract references
Client Name	State of Georgia, Georgia Technology Authority
Contract Title/Contract Reference Number	Title: Managed Network Services Contract Number: GTA MA# 132126UA

AT&T CONTRACT 2 – STATE OF GEORGIA

Primary Contact, Title and Telephone Number	Dean Johnson, Chief Operating Officer, (404) 463-4409
Contract Dates	January 2016 – December 2020; three additional 1-year renewal options
Contract Amount	$275,000,000
Type of Contract (Public/Private Sector)	Type of Contract: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(3) Network Services
Length of Relationship with Client	7 years

Description

In November of 2015, AT&T was awarded the State of Georgia Enterprise Technology Services (GETS) Managed Network Services (MNS) outsourcing contract. AT&T began providing full management of network services for the State of Georgia under the first GETS contract in May of 2009. The towers of service covered by the GETS MNS contract are WAN, LAN, remote access, managed security, and voice services. AT&T supports the GETS MNS contract with a dedicated Life Cycle Management (LCM) team and a dedicated account team of more than 80 AT&T resources. These resources average 15+ years of experience in supporting large managed network engagements like GETS.

Service Framework 3 – **Network Services.** The GETS MNS contract supports a completely outsourced environment for 14 enterprise agencies for WAN, LAN, WLAN, voice, managed security, and remote access services across 159 counties and 58,000 square miles in Georgia. Services are provided using an ITIL/ITSM framework that includes 1,800+ MPLS connections and 100,000+ voice ports statewide. In addition, AT&T manages 700,000+ IP addresses, 3,000+ switches, 1,700+ routers, 400+ wireless access points, the DNS/DHCP environment, and LAN cabling/wiring statewide.

Specific network services that AT&T currently provides to the State of Georgia include transport, router management, managed Internet access, site-to-site VPN, network cloud-based security, managed IPAM\DNS\DHCP, network switching and routing, wireless networks, network authentication, remote user VPN, and managed voice services.

AT&T CONTRACT 3 – STATE OF TENNESSEE

Customer Reference Number	3 of 5 AT&T contract references
Client Name	State of Tennessee
Contract Title/Contract Reference Number	Title: NetTN Contract Number: FA-09-25220 Edison ID 2904
Primary Contact, Title and Telephone Number	Joe Huertas, Executive Director, (615) 770-1126
Contract Dates	July 2008 – June 2018
Contract Amount	$503 million
Type of Contract (Public/Private Sector)	Type of Contract: Firm Fixed Price

AT&T CONTRACT 3 – STATE OF TENNESSEE

	Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (3) Network Services
Length of Relationship with Client	More than 50 years

Description

In 2008, AT&T was awarded the NetTN contract for telecommunication services. This contract includes data network products and services that support the statewide10 Gbps backbone infrastructure—using Multi-Protocol Label Switching (MPLS) to facilitate secure, redundant, high-performance Wide Area Network connectivity. The NetTN network provided by AT&T is a fully meshed network and accommodates various access methods such as private line, Metro Ethernet, and wavelength services. AT&T supports the NetTN network and contract with a Life Cycle Management (LCM) team of more than 30 AT&T resources. These resources average 15+ years of experience supporting large network engagements like NetTN. The team is organized by function, with a Director of Architecture managing engineering and architecture and a Director of Operations who manages provisioning, incident, billing, and other functions.

As part of this contract, the State of Tennessee can order Primary Rate Interface (PRI), Centrex, and local private lines that can support voice signaling, 1FBs (flat business lines), hosted VoIP, and IP Flex Reach. The State currently has approximately 85 PRIs operational today, along with about 5,000 Centrex stations and 3,000 1FBs provisioned statewide. AT&T recently installed two IP Flex trunks and is in the process of testing the trunks' calling features and redundancy options, including linear re-route.

Service Framework 1 – **Service Desk Services.** Identified State of Tennessee users receive Tier 1 Help Desk services from AT&T on a 24x7x365 basis. For those users, AT&T supports managed NetTN and 1FB services.

Service Framework 3 – **Network Services.** Specific network services that AT&T currently provides to the State of Tennessee include circuit to the customer premises, managed router services, Internet access, managed firewall security to and from the Internet, managed intrusion prevention and intrusion detection to and from the Internet, connectivity to all other sites on the NetTN network, Internet2 for eligible entities, and proactive network management and monitoring.

The design of the NetTN MPLS network allows each customer's data traffic to travel a Virtual Private Network (VPN) path from the point of entry into the network to the final destination. MPLS allows for the coexistence of all Government, education, eHealth, 911, and non-profit organizations on the network, along with providing the products and services needed to support new technologies and multiple options for connectivity, performance, and quality of service. Customers can control which of their offices are allowed to communicate with other customer offices and those that must maintain complete separation. AT&T designed and constructed the NetTN network to accommodate data, voice (VoIP), multimedia, and video over the same access circuit. Differentiated Services (DiffServ) within the network provide end-to-end IP Quality of Service (QoS) features. AT&T designed NetTN for 99.999% accuracy at the core and 99.95% accuracy at the end sites. Customers can order Internet service from T1 to 1Gbps.

AT&T also provides managed LAN services to Tennessee 911 at 140 sites where AT&T manages LAN switches in support of the next-generation 911 call routing application. At each of these sites AT&T provides the equipment, management, monitoring, and maintenance. The 140 sites are spread across the

State of Tennessee. AT&T also currently provides Layer 3 Managed LAN (MLAN) services along with the associated equipment, management, monitoring, and maintenance at each of 260 K12 sites.

AT&T CONTRACT 4 – STATE OF MICHIGAN

Customer Reference Number	4 of 5 AT&T contract references
Client Name	State of Michigan
Contract Title/Contract Reference Number	Title: State of Michigan WAN Contract Number: 071B5500011
Primary Contact, Title and Telephone Number	Anne Fisher, AT&T Account Manager, (248) 631-8282 State of Michigan requires initial contact with the AT&T Account Manager who will coordinate a reference call with the State of Michigan.
Contract Dates	October 2014 – October 2019 with five 1-year renewal options
Contract Amount	$82 million
Type of Contract (Public/Private Sector)	Type of Contract: Firm Fixed Price Sector: Public Sector
Services provided (relate to County Service Frameworks in this RFP)	(1) Service Desk Services (3) Network Services
Length of Relationship with Client	13 years

Description

AT&T has been a valued partner to the State of Michigan for years. AT&T held the original WAN contract with the State of Michigan as part of the Master Link Michigan contract from 2003 to 2014, which was worth $132 million. The WAN part of this contract provided the State of Michigan with a custom-managed WAN. The State released a WAN RFP in 2014. AT&T was awarded the Service Integrator, WAN Provider, and Internet Service Provider (ISP) roles.

Service Framework 1 – **Service Desk Services.** AT&T's custom help desk for the State of Michigan provides Tier 1.5 through Tier 3 support for WAN trouble and support issues. Operating 24x7x365, the help desk monitors, manages, and maintains the WAN routers at all State locations. AT&T tools open most trouble tickets automatically, but customers can call the help desk directly to open a ticket. The State receives notification of every auto-generated ticket. AT&T works tickets in accord with the State's contract requirements. AT&T monitors the tickets closely for resolution and any needed escalations. The help desk coordinates and works with all Michigan Local Exchange Carriers, third parties, and ISPs who are part of the State's WAN. AT&T compiles monthly performance reports and reviews them with the State. SLAs govern ticket handling and mean time to repair.

Service Framework 3 – **Network Services.** Under the original contract, the WAN transport was frame relay with a private backbone. During an 11-year period, AT&T migrated 200 locations to AT&T Ethernet services and modernized and enhanced the overall network and operations. AT&T is currently migrating the State from frame relay to a Virtual Private Network (VPN) with Ethernet access. Network products and services that AT&T currently provides to the State of Michigan include VPN, managed

Internet, switched Ethernet, IP broadband, custom managed services, routers, equipment sparing, IP address maintenance, and monthly performance reports.

AT&T CONTRACT 5 – STATE OF CALIFORNIA

Customer Reference Number	5 of 5 AT&T contract references
Client Name	State of California – Department of Technology
Contract Title/Contract Reference Number	Title: CALNET 3 Contract Number: – Agreement No. C3-B-12-10-TS-01
Primary Contact, Title and Telephone Number	Renato Peruzzi, Senior Telecommunications Engineer, (916) 657-9209
Contract Dates	March 2014 – June 2018 (plus extension option)
Contract Amount	Approx. $250 million
Type of Contract (Public/Private Sector)	Type of Contract: Firm Fixed Price Sector: Public Sector
Services provided (relate to Service Frameworks in this RFP)	(1) Service Desk Services (3) Network Services
Length of Relationship with Client	More than 50 years

Description

CALNET 3 is a recent competitively bid contract that provides a comprehensive array of telecommunications and network services for use by public entities throughout the State of California. All State of California Government Agencies can use CALNET 3. AT&T was awarded contracts in seven major service categories. This allows AT&T to provide a wide portfolio of products and services, including integrated, end-to-end solutions across all service categories. It also allows AT&T to help customers transform from legacy services to IP services in an integrated, intelligently planned, and phased migration. Ongoing reviews of pricing and service functionality will assure California that CALNET 3 rates and services remain cost-effective and technologically competitive throughout the life of the contract.

Service Framework 1 – Service Desk Services. AT&T provides, on a 7x24x365 basis, a Customer Service Center. The Customer Service Center focuses on customer support, trouble resolution, and documentation for all CALNET service issues. The Center provides timely responses to reported service issues or the escalation of any previously reported problems, status on trouble resolution and the causes of network or individual service outages, and a toll-free number as a single point of contact.

AT&T must answer 80% of the customer calls–using an automated system or live operator–within four rings. AT&T's live technician must begin collecting information from the customer within 5 minutes of initially answering the call or a customer opening an online ticket. Center personnel must open, monitor, and update trouble tickets using a Trouble Ticket Reporting Tool. Trouble ticket life cycle management includes the initial customer trouble reporting date and time and AT&T's response to the customer; an acknowledgement of the receipt of the trouble ticket, and beginning resolving the customer's service issue within 30 minutes. For SLAs based on outage duration, the duration begins upon the opening of a ticket. AT&T updates the ticket with the status every hour and as soon as service is restored. AT&T's Trouble

Ticket Reporting Tool and trouble ticket content are accessible 7x24x365 via a web-enabled application. AT&T provides notification within 60 minutes for significant and catastrophic events and status every 60 minutes. AT&T also provides support procedures for natural disaster events.

Service Framework 3 – **Network Services.** Network services that AT&T provides to the State of California include transport services, MPLS VPN, converged and standalone VoIP, web conferencing, Metro Ethernet, Synchronous Optical Network (SONET), managed Internet, hosted Interactive Voice Response/Automated Call Distribution (IVR/ACD), network-based security, Service Level Agreements, a billing platform with invoicing and reporting capabilities, and a custom portal program.

HPES Service Framework Additional Reference Information – We have provided below additional Service Framework details for each of our five HPES references.

HPES CONTRACT 1 – COUNTY OF SAN DIEGO

Service Framework Categories of Service Details	
Customer Reference Number	1 of 5 HPES contract references

Service Framework 1 – **Service Desk Services.** Our HPES single point of contact (SPOC) Service Desk provides the County with around-the-clock response to incidents; service requests; and requests for information by phone, mobile phone, email, fax, and web-based portal. We use ITIL-aligned processes to meet all requirements, achieve 70% first-call resolution, and maintain 12-minute resolution time. Our agents own and track tickets and Service Requests (SRs) end-to-end, and those tickets are escalated throughout the tiers.

Service Desk Performance

We exceed all of the County's service levels for our Service Desk:

- First-call resolution rate is more than 70%, and the industry average is 63%.
- Initial call phone handle rate is 7 minutes, 5 minutes less than the requirement.
- Call abandonment rate is 3%, and the industry average is 5%.

Service Framework 2 – **End User Services.** HPES maintains more than 800 servers; more than 15,000 desktops, laptops, and tablets; 1,100 network printers of various sizes; 200 wireless access points throughout the County; and 500 NetMotion-equipped mobile devices. We are also responsible for complete backup, recovery, disaster mitigation support, system controls to monitor network access, system applications, data security, systems monitoring, and end-user services and support for continuity of operations (COOP) services. We manage the desktop client of the County's Lync 2013 messaging environment, serving 16,000 users. Currently, we use Symantec Endpoint Protection 2012 as our anti-virus and anti-malware solution for workstations and laptops and HP ePolicy Configuration Manager (ePCM) for all County servers.

We apply the County's requirements and customizations on a gold disk image for use on servers and desktops. Our team designed and supports the County's Unified Messaging solution, enabling County executives to have their voicemails transcribed into text. We use SCCM for software pushes to County desktops and laptops, and we use HP Server Automation to manage more than 800 County servers. Also, we provide disk encryption and endpoint (tablet, laptop, and desktop) security using Symantec's Endpoint Protection solution. We provide VPN solutions using NetMotion, which is SSLVPN with application persistence in the data centers, and Pulse Secure VPN.

Service Framework 3 – **Network Services.** We manage and support a Microsoft Public Key Infrastructure (PKI) solution for County wireless devices and use Verisign and Entrust certificates for enterprise devices. Our team manages and operate the County's Microsoft Exchange farm and mail relays, which receive nearly 2.7 million emails per week. We operate and manage the County's PBX and

Avaya Voice over IP (VoIP) solution. In addition, we provide infrastructure support for Lync, Webex, and Granicus web conferencing and County-wide broadcasts.

Service Framework 4 – **Data Center Services.** Our data center infrastructure service focuses on performance, availability, and security. We manage and maintain the County's server, storage, backup, network, and security environments. Our services include operating system (OS) patching, ongoing maintenance, and performing all database and application installations. Our processes determine impacts to data center-resident critical business components and systems to continuously analyze them. We identify and remediate single point failures using root cause analysis and corrective actions for physical and virtual servers, as well as storage, backup, and network problems. We provision the County's servers in accordance with County requirements.

Currently, we manage the Exchange 2010 High Availability environment, mailboxes, OWA traffic, and RightFax solution. HPES designs, deploys, and maintains software distribution for desktop computing services and integrates and performs software delivery for County mobile devices.

We manage and support the County's Active Directory (AD) forests, one for the County proper and one for the Public Library. We host them in two client-managed facilities and two HPES data centers, which provide failover capabilities in case of disaster. We manage print servers and EMC Celera file servers within our data centers. In our County-serving data centers as well as locally in San Diego we back up all of the County's UNIX and Windows servers using HP Data Protector writing to HP Virtual Tape Libraries. We manage and host DHCP services for all of the County facilities within the data center. HPES manages external and internal AD-based Domain Name Services (DNS).

We provide approximately 1.5 PB of storage for the County. Our storage services provide the County with Network Attached Storage (NAS), Storage Area Network (SAN), tiered, and immutable storage options. NAS services provide tiered storage for home and group shares. SAN services provide storage for physical servers, VM hosts, and NAS appliances. We use Write Once Read Many (WORM) storage appliances to provide immutable (offline) storage services. We back up all of the County's storage using HP Data Protector writing to HP Virtual Tape Libraries.

HPES is a non-voting member of the Security Governance Committee and contributes to development and monitoring of security procedures. For storage, information processing, data handling, network transport, and Internet access, we maintain a posture that aligns with the County's goal to secure and protect IT resources and with industry standards. We provide identity management, federated access, and secure mobility solutions

Our Security Operations Center (SOC) gathers feeds from the County's Security Information and Event Management (SIEM), firewalls, and Intrusion Detection/Intrusion Prevention system (IDS/IPS) devices for event alerts and notifications—reporting the issues to the County CISO regularly. We manage 16 CheckPoint and Juniper firewalls. HPES uses HPE Tipping Point and Juniper IDS/IPS appliances. We manage the County's Websense proxy and content filtering solution. Also, we manage an HP ArcSight solution that collects feeds from its firewalls and IPS devices for event logging and threat correlation. We perform annual penetration testing using Metasploit software. In addition, we provide remediation and mitigation, including policy pushes for all security devices, security patching, and vulnerability remediation based on security scans. We provide forensics services through our Digital Investigation Services (DIS) team.

Our engineering processes incorporate Information Assurance (IA) into the design, engineering, builds, monitoring, administration, patching, and repair of the County's entire IT infrastructure. IA features of our design, development, testing, and implementation services include anti-virus for workstation and servers using Symantec and patch management for Solaris, LINUX, and Windows server and Windows workstations operating systems. We incorporate IA into our Oracle and SQL databases and applications.

These IA features include review of various threat notification sources, including preventive actions, mitigation, remediation, and intrusion detection and prevention using Juniper and Tipping Point; security event correlation and log retention using ArcSight; vulnerability management, including penetration tests using Nessus and Metasploit; email protection for spam and malware; virus protection for mail gateway and internal email using Ironport and Forefront; forensics investigation; and incident response services, including investigation, containment, mitigation, and remediation. Our security authentication services helped improve integration across the enterprise; single sign-on helped improve efficiency. We also implemented advanced anti-virus software with heuristic detection and added firewall and intrusion prevention software to all County end-user computing devices. This lowered the infection rate by more than 90%, which improved up-time for the County.

HPES manages and operates the County's Microsoft Exchange farm and mail relays, which receive approximately 2.7 million emails weekly. We manage the County's Lync 2013 messaging environment and provide the infrastructure support for Lync, WebEx, and Granicus web conferencing and County-wide broadcasts.

Since 2010, HPES has provided managed print services from the County print room located in Rancho Bernardo. Our print operations processing takes place Sunday through Friday from 8:30 p.m. to 2:00 p.m., PT, with on-call support available. With the transition of the Juris managed print requirements to Fujitsu, we will continue to provide managed print services of approximately 200,000 pages per month to meet assessor and tax collector requirements, from our print facilities.

Service Framework 5 – **Application Services.** We monitor the health of more than 400 steady-state business applications and assist in troubleshooting infrastructure issues. We provide total application support as needed for the various application types. Also, we provide database administration and development support for Oracle and SQL database for all of the County applications. We manage the County's Active Directory (AD) Federated Services and Oracle Identity Management. HPES provides a complete managed Citrix stack to optimize applications over the County-wide WAN.

Application Services Achievement

HPES achieved a 100% rating on all Priority-1-under-4-hours application service calls.

Applications Development – Jointly developed by HPES and CTO the Justice Enterprise Library System (JELS) is an application that eliminates paper, supports more effective case management, and streamlines courtroom proceedings. Developing JELS was an enormous undertaking. It needed to accommodate more than 1.3 million documents that come from a wide variety of sources and in a wide variety of file formats. A number of separate organizations—district attorney, probation, public defender, alternate public defender, and separate County contract panel attorneys—needed access to it. JELS had to meet the DA Office and the other County attorneys' needs both functionally and in terms of ease-of-use.

JELS Positive Outcomes

- Increased efficiency – helps clear juvenile court dockets and speed processing of juvenile offenders.
- Increased accessibility – files are now available immediately, anywhere, anytime.
- Increased flexibility and mobility – eliminates old worries about who can use paper files and when.
- Increased security – working off-site no longer puts files at risk; case files are now backed up.
- Reduced the risk of losing documents, which also improved attorneys' peace of mind.
- Reduced the county's paper purchasing costs by $50,000 per year.

HPES took an iterative, Agile development approach, which gave attorneys the opportunity to provide input incrementally. Pieces were developed and deployed in short time frames, worked with in the live environment, and modified if needed. The result of this teamwork was a platform that the attorneys

quickly embraced. JELS is built on Microsoft SharePoint and leverages that software's site creation, document library, and workflow features.

However, unlike most SharePoint deployments, which typically focus on document storage, JELS also supports user-friendly, in-court use of these documents. Called an "e-briefcase," this feature lets attorneys easily copy electronic case files onto their laptops. The e-briefcase files are searchable, and they can be amended using Adobe Acrobat. Attorneys can also append notes to them, which is helpful for maintaining their confidential records of court proceedings. JELS is also highly secure. Each organization that has access to it works through its own, dedicated web portal. This makes certain that information generated by, the DA Office for example, cannot be viewed by other JELS users, such as the public defender, a possible adversary.

Applications Rationalization – In 2011, the County engaged HPES to conduct a comprehensive applications rationalization. There were multiple drivers for the project, ranging from the need to optimize the use of funds in a challenging economy to enablement of innovative services, such as mobility. The County had performed applications rationalization in the past on the group-specific applications using a variety of different rationalization methodologies. This time the objectives were to conduct an enterprise-wide rationalization using industry best practices, use standardized methodology and tools, and use tools that facilitated effective analysis and allowed for ongoing portfolio management. A final objective was to educate County staff and implement processes that allowed the County to continuously manage its entire application portfolio.

Our consultants worked with the County application owners during the end of 2011 and the beginning of 2012. The project followed our multi-step Applications Rationalization RightStep methodology, which begins with joint strategy setting and ends with a transformation plan, including business cases. We pulled a lot of County data from different sources, and then we mapped and loaded it into our Application Portfolio Manager (APM) tool. Some of the data was old, and its quality was unknown. Rather than relying on it as it was, we used the built-in workflows in APM to conduct a data validation cycle—bringing the metadata for all of the applications in the portfolio to a consistent, high-quality level. To capture stakeholder and user assessments of how applications perform from a functional and technical standpoint, we sent more than 2,000 surveys with more than 20 questions. Then, we consolidated the responses in the APM tool.

Two critical areas for successful application rationalization are mapping of applications to business processes and determination of application inter-connections. In both cases the information in the County was only partially available and not consolidated. The models we built in APM captured the County business processes to Level 3 or Level 4 and described all of the linkages and interfaces in the system architecture. Connectivity between applications had traditionally been documented in each application design document, but there were several gaps. We used the dynamic graphing capabilities of APM and gathered experts around huge wall charts to debate, investigate, and correctly document how applications fed information to each other. Then, we looked for areas of overly complex interconnectivity that were targets for simplification, which reduces maintenance cost and increases agility.

Apps Rationalization Outcomes:

- Laid out 14 specific initiatives with business cases in a proposed roadmap demonstrating ways for the County to reduce costs, increase agility, and decrease risk
- Identified more than 25% of the portfolio as retirement candidates
- Enabled County staff to continuously manage the application portfolio using our APM tool.

We used application metadata, application scores (from the surveys), application-to-business process mapping, and application-inter-relation mapping as inputs to the APM's analytical capabilities.

Application-to-business process mappings helped us to identify applications that supported very few (or no) business processes as well as business processes that consumed a high number of applications or none at all. The project identified several opportunities to improve the application portfolio. Some examples included consolidation of applications with functional overlap, technology refresh to avoid skills or technology risk, and pockets of overly complicated integration structure contributing to a high cost of change. We delivered project recommendations to the County in March of 2012.

Enterprise Web – The County needed a centralized platform to host all of its public websites and provide enterprise-grade web content management. We responded by building a solution based on Adobe Experience Manager to provide an environment to create, manage, and publish public websites. Adopted by County business groups and the Board of Supervisors, our solution established a standard platform as the target environment to which the County is migrating all of its legacy websites.

Sandiegocounty.gov is now supporting 14 million hits per week; 70% of those hits are being served from Akamai—reducing bandwidth requirements. The platform supports multiple form factors—laptop, desktop, tablet, and smartphone.

Mobility – The County wanted to improve probation officer effectiveness in reporting their field assessments, case planning, and supervision and case management activities. Probation officers needed tools to increase their face-to-face time with probationers. In addition, probation officers needed a way to identify targets and collateral individuals in a timely manner. Lastly, the County wanted to support California's criminal justice system realignment—thus increasing local level supervision of people convicted and now on probation.

In response, we identified the core business functions that the County wanted to migrate to a mobile platform, along with key dependencies. Then, we built a secure system that provides the probation officers with the mobile ability to work online and offline; connectivity issues do not prevent the application from functioning. The system provides five layers of security for PO authentication.

Some of the Mobility project's outcomes are as follows:

- First in the industry to mobilize probation officer case load
- Provides complete and timely information at probation officers' fingertips
- Increased probation officer productivity by 54%
- Probation Officers are now spending more time in the field and less time back in the office performing data entry.

Probation Officer Mobility Project Outcomes

- First system in the industry to mobilize probation officer case load
- Provides complete and timely information at probation officers' fingertips
- Facilitates better and more meaningful contact notes
- Allows probation officers to spend more time in the field and less time in the office entering data
- Increased probation officer productivity by 54%
- Improved parent involvement in developing case management plans.

The system improved parent involvement in developing case plans and receiving progress updates. It increased probation officer efficiency and reporting with better and more meaningful contact notes. The system was awarded second place in the 2015 GovTech Digital Counties Survey. It is described as a positive transformational change in a probation officer's day.

HPES CONTRACT 2 – U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT (HUD)

Service Framework Categories of Service Details	
Customer Reference Number	2 of 5 HPES contract references

Service Framework 1 – Service Desk Services. We staff and operate HUD's help desk and provide Tier 0 (knowledgebase and FAQs) and Tier 1 level support. Our team opens, logs, and tracks tickets and helps users with password resets and lost or expired passwords. They route tickets (problems and incidents) to second-level and third-level support that provides end-user services. The help desk supports desktops and field services through a single call-in number. It services approximately 14,000 HUD users and several thousand of HUD's contractors and external business partners in more than 80 locations throughout the United States and its territories. Our service center solution consolidated HUD's numerous IT support service centers into a single service center that is collocated with the HITS data center. Our solution enabled HUD to eliminate redundant service centers, reduce costs, improve service levels, and reach a single point of contact for incident tracking. We send customer satisfaction surveys to each user who calls the service center. We also survey HUD executive users on a bi-annual basis to make sure that we are meeting customer satisfaction levels.

Our Tier 0 and Tier 1 Help Desk team handles 13,000 – 18,000 calls per month and has consistently achieved customer satisfaction levels of 95% and higher, where users rate the services of HPES as good or excellent. Our service center adopted use of the ITIL framework and incorporates continual service improvement (CSI) in our operations methodology. This continual improvement helps to create an environment that becomes progressively more trouble-free over time.

HUD Service Desk Facts

- Delivers ITIL-based services
- Handles 13,000 – 15,000 calls per month
- Consistently achieves customer satisfaction levels of 95%
- Incorporates Continual Service Improvement (CSI) in its operations methodology.

The service center operates on a 13-hour day, 5-day-a-week basis (excluding Government holidays) to record and resolve user issues and service requests. Calls outside of the service center operating hours flow automatically to an operational command center, which records all issues in the ticketing system for later follow-up and resolution but addresses only significant, critical emergencies outside of the normal service window. Classified as a major application, our service center system has received Authority to Operate (ATO), which Government Agencies grant according to a risk-based framework that analyzes how a vendor has implemented the security controls within their IT environment.

Service Framework 2 – **End User Services.** We manage HUD's wireless and mobile device environment for more than 1,600 end users. Mobile end-user services we provide include setup, monitoring, and administrative services, such as application and access provisioning. We also provide ongoing research, testing of new capabilities and configurations, and Tier 3 troubleshooting services. The specific mobile platforms we support include Blackberry, iOS, Android, and Microsoft Surface devices. During the term of our contract, we have used several different mobile device management (MDM) tools, including BlackBerry Enterprise Server (BES), Good for Enterprise, Good Mobile System Management/Boxtone, and AirWatch. We are now using Microsoft InTune. *From this experience, we understand the strengths and weaknesses of those tools and can share that information with the County.*

Service Framework 3 – **Network Services.** HPES provides network connectivity to the HUD WAN from the HITS data center in West Virginia; the Program Management Office (PMO) in Herndon, Virginia; and six regional HUD offices around the country. We also manage the LAN environment in the

data center. We secure all of the services provided to HUD through our Security Operations Center (SOC). Our security services include firewall management, intrusion detection, anti-virus management, and computer incident response services.

Service Framework 4 – Data Center Services. HPES provides HUD with managed mainframe, midrange, client server, and data center services in our company-owned data center. We provide Disaster Recovery (DR) services using a commercial service provider. We provision, operate, refresh, and maintain our data center hardware environment (Unisys and IBM mainframes; AS400, Sun E10K, UNIX, Linux, and Windows application servers; UNIX, Linux, and Windows web servers; UNIX, Linux, and Windows database servers) and all associated peripherals. We monitor and manage environment system status, process status, and environmental controls, and we perform any necessary actions based on detected problems or issues. Our team manages all third-party supplier contracts, such as rental agreements, leases, service agreements, warranties, amendments, and maintenance contracts. We support open server environments and applications on platforms ranging from mainframe to midrange. We provide and support more than 600 terabytes (TB) of data storage.

HUD Data Center Achievements

- Consolidated HUD's data centers
- Virtualized HUD's server environment
- Established the first large-scale Government private cloud
- Now building a multi-cloud managed environment—providing innovation leadership that enables HUD to increase cloud adoption and optimize management and operation.

We provide and manage the physical security for our facility. We manage access to the data center so that only authorized staff members have access to the facility. We schedule and coordinate periodic evacuation drills. We implemented Integrated Windows Authentication (IWA) to enable Single-Sign-On (SSO) into the service center system and to inherit and enforce agency account and password security policies. A built-in, role-based access control system controls access to service center features. We developed custom workflows to process, approve, and implement requests for updates to accounts and application access.

Service Framework 5 – Application Services. HPES hosts more than 280 HUD applications and provides Disaster Recovery for 35 applications. At contract start we acquired a data center facility that was fully ready to support HUD needs in Charleston, West Virginia. We planned, engineered, coordinated, and executed a flawless transition of HUD's production applications and their development and test environments seamlessly and without interruption. We completed a complex, 6-month transition project on time and under budget. Following weeks of planning, we seamlessly migrated more than 200 applications to our data center without disrupting HUD's operations.

Flawless Applications Transition

- We planned, engineered, coordinated, and executed a flawless transition of HUD's production applications and their development and test environments.
- We completed the complex, transition project on time and under budget.
- We migrated more than 200 applications to our data center without disrupting HUD's operations.

HPES successfully migrated HUD's website HUD.GOV from an outdated technology onto an enterprise content management system that uses document and workflow management of web content. In a similar way we migrated HUD's intranet site HUD@WORK onto a new highly scalable web platform that uses responsive design and HTML5 features.

For mobile HUD users, HPES developed, implemented, and now supports the following apps:

- Fair Housing Discrimination Mobile Application (iOS/Android) – Uses the latest technology to give the public a quick and easy way to learn about their housing rights and file housing discrimination complaints. It also informs the housing industry about its responsibilities under the Fair Housing Act.
- Rebuild Healthy Homes (iOS/Android) – Informs users about the essentials of healthy homes for indoor residential environments following natural disasters. Information covers the principles and technical aspects of the safe and proper removal of mold, radon, asbestos, lead, and other hazards.

In addition, we provide secure web-hosting for an application named Office of Fair Housing and Equal Opportunity (FHEO) Form 903, which provides a back channel to reach citizens through the discrimination complaint application. These mobile applications run on iOS 5.1 or later for iPhone, iPad, and iPod Touch; they also run on Android devices. We used the following technologies to build these applications: JSON, XML, RESTful, Objective-C, Java, and Secure Sockets Layer (SSL). The backend web-application runs on Oracle WebLogic Server 11g.

HPES CONTRACT 3 – U.S. DEPARTMENT OF NAVY

Service Framework Categories of Service Details	
Customer Reference Number	3 of 5 HPES contract references

Although the Next Generation Enterprise Network IT (NGEN IT) enterprise is larger and more complex than the County's enterprise, the IT services and support requirements are similar. The tools we use are similar. The service level requirements are similar.

Service Framework 1 – **Service Desk Services.** HPES has consolidated and standardized Information Technology Infrastructure Library (ITIL)-based network operations, security, and user assistance across every level of service. HPES and DoN designed, developed, deployed, operates, and maintains four fully integrated enterprise Service Desks—in Norfolk, Virginia; San Diego, California; Boise, Idaho; and Hawaii—handling 1.9 million calls per year. The Service Desk provides a single point of contact for resolution of incidents, end-user assistance for standard IT questions, and service requests. Service Desk services include technical support assistance, service request management, business request documentation, remote desktop management, self-help tools, and hardware/software that directly supports the service desk and that is not common to other defined services (e.g., the trouble ticket management system).

The Service Desk supports users with the following types of requests and support situations:

- Support for common, standard user workstations and associated software (standard/ common configuration/ build) deployed throughout the environment
- User authentication and password reset requests
- Support for wireless devices and users
- Specialized support for classified and unclassified user devices and applications employed within a classified environment or on a classified network
- Mission-critical level of support for specific situations that require stricter service levels.

Service Desk Improvement

By implementing Tier 0 (self) services we reduced Service Desk wait times by 50%.

The Service Desk handles 97,000 contacts per month with 84% first-call resolution (FCR) rate. It processes 51,000 moves, adds, and changes per month. It monitors 53 Service Level Requirements (SLRs) composed of 177 separate metrics. Two of the tools we use are HPE Service Manager (HPSM) and Good for Enterprise (for mobile device management).

Service Framework 2 – End User Services. We and the DoN manage 230,000+ Navy devices, including approximately 22,000 mobile devices. We manage VTC services from 525 end points and the delivery of 33 million+ email messages weekly—incorporating 20 TB of data daily. We and our partners perform all of the design and refresh work associated with end-user devices such as desktop computers, laptop computers, and peripherals. We provide Tier 2 deskside break/fix support for 985 VIP and 82 executive VIP users. In addition, we conduct regular technical support surveys to verify that end users receive effective, efficient service and identify areas for continual process improvement (CPI).

High Satisfaction with End-User Services

The most recent survey for our end-user Field Services shows high satisfaction, with an average score of 4.35 out of 5 (5 meaning 100% satisfaction), with 47% of responders giving us a perfect 5 score.

"HPES consistently delivered specified patches and updates for mobile devices reliably and without error. During this period, the Program Office initiated a transition from BlackBerry to an iOS based mobile device capability that required changes to both devices and device management capabilities. HPES provided solutions that accurately loaded required software and configuration policies to end user devices 100% of the time on the first try."

Navy end users can use Government-furnished iPhones running iOS8 to access their NMCI email, calendar, contacts, and web-browsing. The new platform complies with appropriate DoD regulations and is accredited for use with the NMCI network. We expect to further expand the platform to support more devices, including Android-based phones and tablets.

The Tier 1 Full-Service Printing Service is one of three levels of end-user printing services that we offer on the NGEN contract—Tier 1, Tier 2, and Tier 3. Tier 1 service allows users to have the right devices in the most convenient locations. The goals of the service are to increase efficiency, reduce the visible and hidden costs of imaging and printing, right-size the enterprise by standardizing on fewer printer models, and have the ability to enforce print standards and policies. We deliver that end-user service at a fixed price in print volume increments of low, medium, and high. The low-volume option supports 10,000 – 40,000 pages per month, medium supports 10,000 to 40,000 pages per month, and the high-volume option supports more than 40,000 pages per month.

Service Framework 3 – Network Services. We manage daily operations and network security and perform end-to-end monitoring, management, maintenance, and administration for all NMCI NGEN services and infrastructure. Our areas of support include wireless, video, voice, boundary, and demilitarized zone (DMZ) services. Our video teleconferencing (VTC) services consist of the hardware, software, network, and scheduling services necessary to deliver real-time video and audio communications between end users at two or more of more than 525 VTC end-point locations.

Convenient Print Services at a Fixed Price

- Allows users to have the right devices in the most convenient locations
- Delivers products and services at a fixed price in low-, medium-, and high-volume increments.
- Includes hardware with full support through warranty and break/fix, initial hardware configuration and setup, network printing operations and maintenance, Original Equipment Manufacturer (OEM) consumables (e.g., toner), and full life cycle management.

Our network engineering team conducts solution research, development, and support for the NMCI NGEN network infrastructure. They apply technology changes and updates. They oversee implementation of 400+ VPN/Wide Area Network (WAN) changes and 600 classified Base Area Network (BAN) changes annually. The current network infrastructure consists of 75,000+ network devices and supports more than 10 terabytes (TB) of data flowing across the network per day.

We implemented a wireless Local Area Network (WLAN) and classified WLAN solution, a wireless bridging solution, and a microwave solution that handles greater distance needs. We have consistently delivered video teleconferencing (VTC) solutions for unclassified and classified data, supported voice over Internet Protocol (VoIP) systems, and offered our own IP telephony and VoIP capabilities.

Continuous Network Improvement

We initiated a creative solution to significantly free up traffic flow to and from the Network Operations Center (NOC), resulting in faster browser and email load times while providing more reliable network connections.

As a result, the transport boundary utilization dropped load times from 70% to 14%. Additionally, the site's traffic freed more than 400 MB in bandwidth capacity.

To support a global network constantly under attack we developed a defense-in-depth solution that integrated several technologies with the architecture. As part of our security services, we integrate and correlate data across NGEN systems, servers, services, and end points to measure, monitor, remediate, and remove threats to the environment. We implement, operate, and maintain IA capabilities, including Network Access Control (NAC); anti-malware appliances, hardware, and software; Host-Based Security System (HBSS) and supporting infrastructure; anti-spam; and mail filtering. We also correlate data and manage information from all IA sensors and devices to help us analyze information systems and networks, and we identify potential security weaknesses and exposures to known threats.

Service Framework 4 – **Data Center Services.** We manage 4,400 enterprise-wide servers and 1,442 virtualized servers running in 10 classified, 25 unclassified, and 30 micro-geographically dispersed data centers. We operate and maintain classified and unclassified storage capabilities, including software, hardware, processes, and tools to facilitate the management and reporting of different classes of storage services across a wide range of workloads and applications.

Service Framework 5 – **Application Services.** We established a centrally managed, secure application hosting environment to support enterprise applications. Our managed hosting support includes solution development, migration/engineering assessment, service preparation and setup, facilities and inventory, server management, client services, database management, application administration, storage management, applications hosting network hosting services, information security services, and Disaster Recovery.

We host approximately 30 of our client's enterprise applications in our secure HPES-owned Application Hosting Facility (AHF). We also host and support all of the applications we use to operate, monitor, and maintain the NGEN enterprise. To date, we have virtualized 83 of those applications, which range in function from print services to email, terminal services, anti-virus, and knowledge management.

HPES CONTRACT 4 – CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION

Service Framework Categories of Service Details	
Customer Reference Number	4 of 5 HPES references

Framework Service 1 – **Service Desk Services.** From 2010 to February 2016 we staffed and managed an on-site multi-tiered Service Desk for CDCR. In February 2016 we began training client staff to run the desk. On March 1, 2016, we completed the transition of Service Desk operation to CDCR. We currently augment CDCR Service Desk staff even after transitioning primary responsibility to our client.

During the 6 years we ran the Service Desk, we supported operations 24x7x365, handling approximately 2,500 tickets per month. CDCR used—and still uses—Remedy for incident tracking and recording. End

users can enter and view Remedy. The CDCR Service Desk has a knowledgebase; context-sensitive, online help; FAQs job aides; and interactive training. Our HPES team members used—and still use—Remedy to support the CDCR Service Desk because it is a contract requirement. However, our HPES team members use HPSM to track outages and issues for internal production operation reporting.

Service Framework 3 – Network Services. We manage the network connections between CDCR's headquarters and our Rancho Cordova Data Center (Rancho Cordova is a suburb of Sacramento).

Modernized Processes Improve Lives

"With the help of HPES, CDCR implemented a successful program that modernized processes and improved the lives of people." -- Former CIO of California

Service Framework 4 – **Data Center Services.** In our data center we support CDCR's database, application, authentication, and report servers for test and production environments. Those servers use Windows, Linux, and UNIX operating systems. We provide multi-node failover services. We also operate the CDCR's storage subsystems, network switches, and monitoring services.

Service Framework 5 – **Application Services.** SOMS enabled the retirement of more than 40 legacy systems. The two primary systems replaced are the Distributed Data Processing System (DDPS) and the Offender Based Information System (OBIS).

As part of the decommissioning process, we converted data from OBIS and DDPS and migrated it to SOMS. This included more than 1 million offender and 2.4 million visitor records. With the decommissioning of the legacy systems, *CDCR is saving millions of dollars in maintenance and operations costs* while securing a centralized, web-based application that provides the access needed to meet CDCR's stated mission and objectives.

HPES CONTRACT 5 – CITY OF ANAHEIM, CALIFORNIA

Service Framework Categories of Service Details	
Customer Reference Number	5 of 5 HPES contract references

Service Framework 1 – **Service Desk Services.** Our Service Desk supports commercial software; custom web-based applications; desktop, laptop, and tablet computers; and printer hardware. Our on-site service desk's operational hours are Monday through Friday, 7 a.m. to 6 p.m., Pacific Time, at which point our on-site operations staff takes over the Service Desk phone. On weekends we use a rotating on-call schedule that supports the client on a 24x7x365 basis in accordance with contracted service response times. Our Service Desk tickets average in the 1,000 to 1,200 per month range. We handle all IT-related requests required by the client to operate, maintain, and expand their business. Our contract is Staff Augmentation, but there is one City staff member on our phone infrastructure support team; all other employees are HPES personnel.

The City uses CA Unified Service Desk as their primary service desk tool; however, they also use an in-house-developed knowledge base in the form of electronic run books to track server infrastructure and related application information. The City's ticketing system includes resolution information that can be searched for problem resolution tasks. HPES is supporting one current project to explore the City's self-help requirements for user-initiated password resets. For mobility service users the AirWatch Mobile Device Management (MDM) tool provides a self-help portal that allows enrolled users to manage their devices without incurring administrator intervention. For another current project, we are helping our client to evaluate MS Service Center or HP Service Manager as a potential replacement for CA Unified Service Desk.

Service Framework 2 – **End User Services.** We provide on-site hardware maintenance support for all City-owned desktops, laptops, tablet computers, printers, servers, switches, and firewalls. In 2014 we helped the City create a Mobile Strategy through our HP Mobile Strategy Consulting (MSC) assessment and roadmap. Our transformation and mobility consultants evaluated the maturity of the Mobility program across several mobility dimensions, established a target state, identified initiatives to transition from the current state to the target state, and provided a high-level roadmap to get to the target state. Our evaluation achieved the following outcomes:

- Recommended how to deal with the missing items (go forward plan/next steps).
- Defined current mobility maturity status at the City of Anaheim
- Documented the mobility desired state
- Analyzed three specific mobility dimensions, including mobile management services, security and compliance, and policies and governance
- Conducted a gap analysis (current state versus desired state).

With our support, Anaheim is currently undergoing an MDM trial deployment at the fire department and is awaiting approval for a trial deployment to the police department. The use of AirWatch software is part of this trial.

Service Framework 3 – **Network Services.** We operate and manage network connections to all 62 City facility buildings and associated structures. The network is built on Extreme Networks' equipment, with some Cisco devices in the mix. We use Palo Alto Advance firewalls to protect the network. The network has redundant connections to two Internet Service Providers (ISPs) using direct fiber connections. Current projects that we manage will refresh the core network technologies in the near future.

Service Framework 4 – **Data Center Services.** We operate and manage the City-owned data center, which houses 420 Intel-based servers—of which 273 are virtualized using VMware. These servers are a mix of Windows and Linux servers. The data center also hosts 800 TB of Storage Area Network (SAN) storage replicated to our HPES-owned Colorado Springs, Colorado, Disaster Recovery site for protection. The City's network core infrastructure resides in the City's data center, as do some IBM pSeries AIX and iSeries (AS/400) servers that are slated for retirement in the near future.

We inventory and track all data center and platform hardware components and changes, including information about hardware shipping and receiving, raised-floor space requirements, equipment placement, cabling, and fiber and connectivity details that make up the compute platform environment. We coordinate all hardware configuration changes through the site's change management process. In addition, we document and track all hardware configuration management problems using the site problem management process and work with suppliers to identify and implement short-term fixes to eliminate the immediate problem. Then, we identify permanent corrective actions to eliminate the fault from the environment.

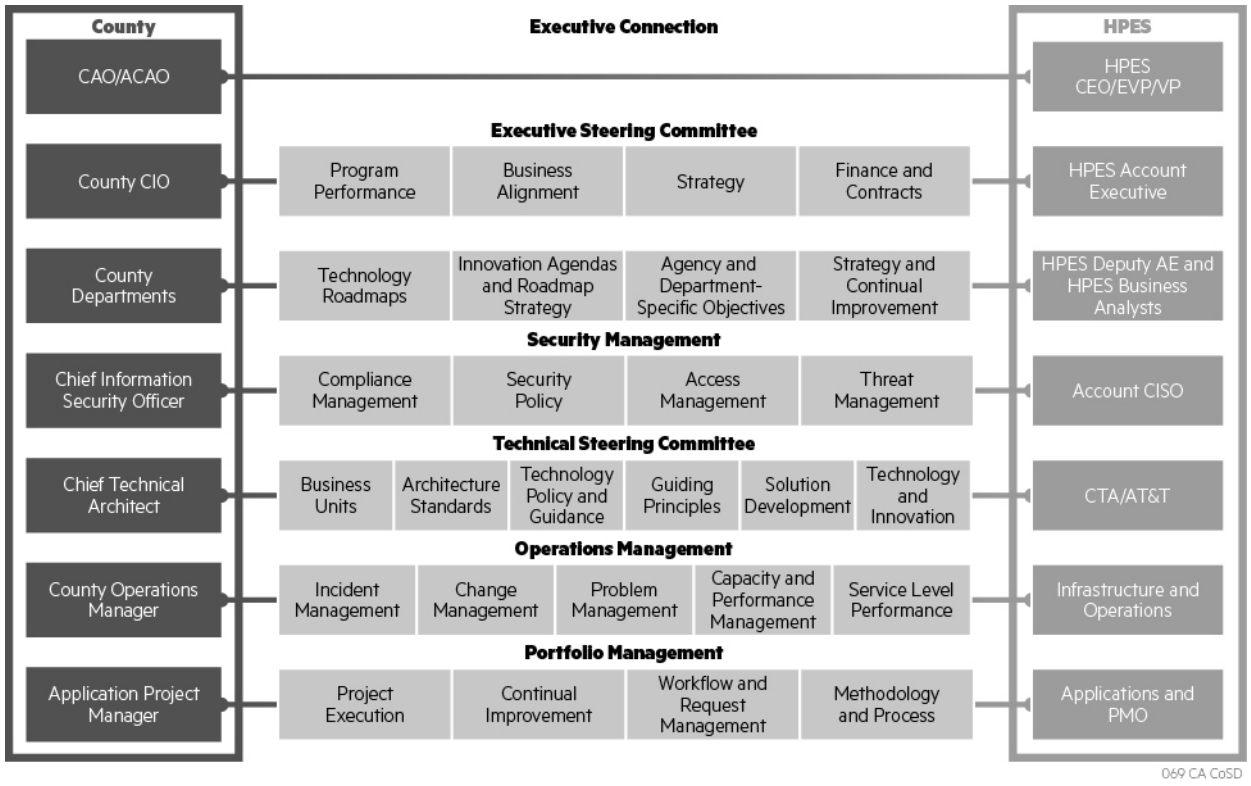
Service Framework 5 – **Application Services.** HPES supports approximately 100 applications for the City. The applications range in size from small MS Access applications to large enterprise class applications, such as Enterprise Resource Planning (ERP) and Customer Information System (CIS). EnQuesta—which processes and electric and water meter reads—turns them into bills, issues invoices, deals with payments, and the like. Our services range from support for COTS applications (patching, issue resolution, upgrades, interfaces, and reports) to application development and support (requirements gathering, development, testing, and implementation).

2.3 Offeror Response to Organization and Staffing Questionnaire

2.3. Offeror Response to Organization and Staffing Questionnaire

HPES has implemented a multi-tiered interactive framework for communication and decision-making that provides effective collaboration and timely action. This framework, illustrated in Figure 1, maximizes communication based on the County's organizational structure. HPES and County leaders are aligned to the framework in such a way that we can produce results consistent with technical and process architectures. From requirements definition to solution implementation, this organizational alignment fosters solid understanding of business needs and effectively identifies opportunities for innovation and process re-engineering. The HPES leader puts into motion collaboratively developed plans of action based on agreed decisions to achieve the best outcome with world-class services to your citizens. We will work with you to align ourselves to the existing governance within the County Technology Office (CTO) and business groups.

Figure 1. Multi-tiered Interactive Framework for Communication



Our interactive communications framework aligns HPES and County leaders to achieve solid understanding of business needs and identify opportunities for innovation.

Our County organizational structure achieves the best balance of economy and effectiveness by assigning senior staff to lead functional area teams. These teams of highly qualified experts—with more than 20 years of combined experience supporting the County—possess detailed knowledge of County business, which results in effective, collaborative interactions with County staff. These interactions help everyone to focus on moving from Idea to Value as quickly as possible.

2.3.1 Overall Organization Chart

2.3.1. Describe your total organization, including any parent companies, subsidiaries, affiliates, and other related entities. Provide an organization chart.

Effective November 1, 2015, HP Enterprise Service's former corporate parent, the Hewlett-Packard Company (HPCo), separated into two publicly traded Fortune 50 companies. One company comprises HPCo's enterprise technology infrastructure, software, and services businesses and is now an independent, publicly traded company, the Hewlett Packard Enterprise Company (HPE). The other company, HP Inc. (formerly known as Hewlett-Packard Company), comprises HPCo's printing and personal systems businesses and retains the HP logo. As part of the planning for this transaction, HPCo took steps to maintain the strength and reliability of HP Enterprise Services, LLC, and other entities.

HP Enterprise Services, LLC (HPES), is a fully owned subsidiary of HPE. [HPCo stated in its 2014 Form 10-K] that, based on HPCo's fiscal 2014 results, excluding Corporate Investments and intercompany elimination, HPE will have planned segment revenue of $57.6B. HPE is well capitalized and is expected to have investment grade credit ratings. HPES is presently unaware of any plan to change the present structure of HPES as part of the separation that would require HPES to seek a novation of the contract, if awarded one.

A copy of the HPES overall organization chart is located in Volume IIA – Confidential/Proprietary section of this volume.

2.3.2 Proposed Staffing Organization Chart

2.3.2. Provide an organization chart of your proposed staffing at a role level (e.g., desktop technician, service desk agent), showing reporting relationships to provide the Services described in this RFP, including the Prime and Subcontractors, from Account Executive and broken down into Service Frameworks.

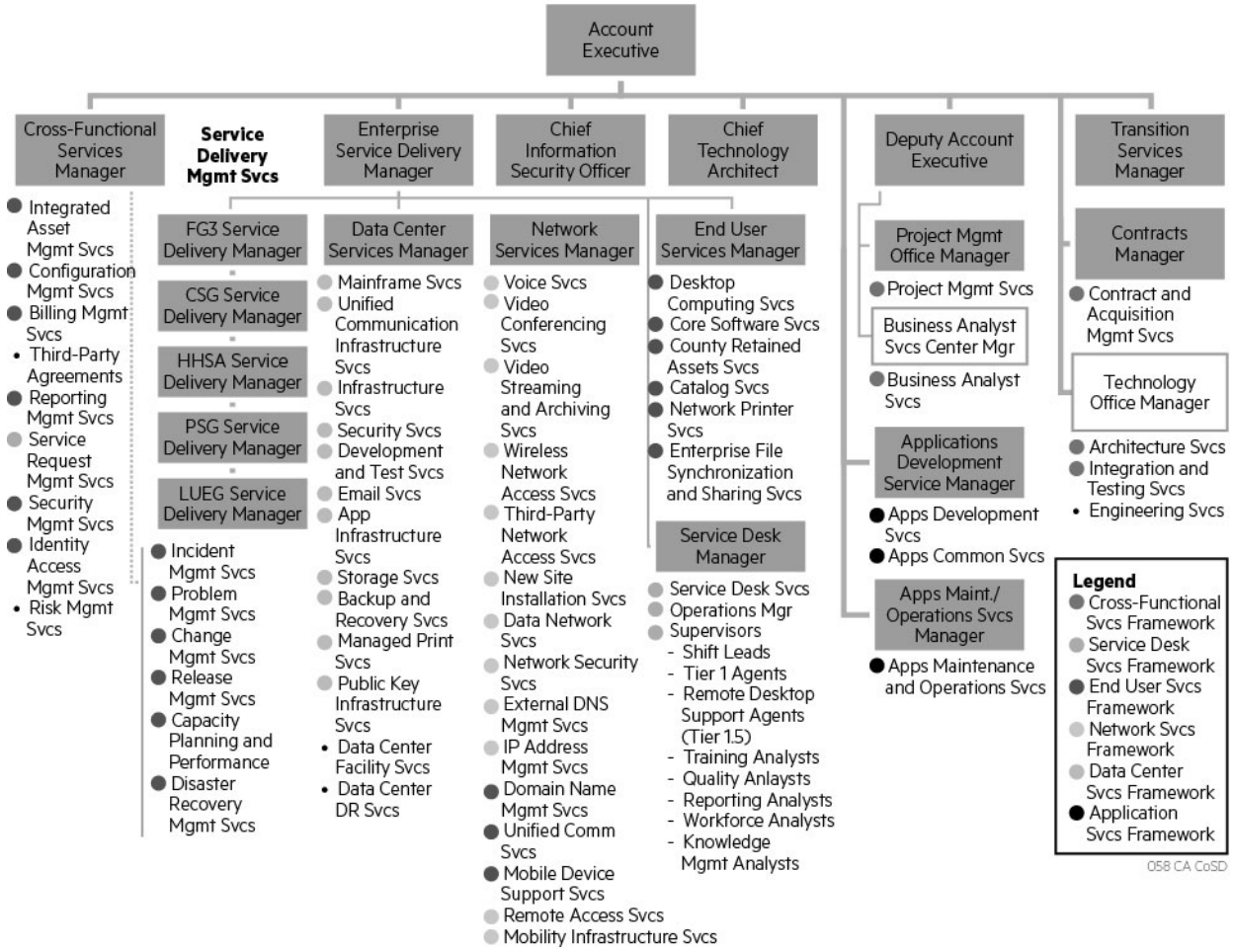
High-caliber, experienced team ready Day One = Continuity of resources for lowest-risk transition

The County of San Diego will experience an immediate, non-disruptive transition to the new information Technology Outsourcing (ITO) contract because HPES has been supporting the ITO since 2006 and has served as prime contractor since 2011. This makes us ready on Day One to continue delivering ITO support services at the lowest risk.

With HPES, the County will retain resources with critical institutional knowledge of your IT environment because our in-place account team includes ~300 personnel supporting the contract today, including 20 employees identified as Key Personnel.

We have provided an organization chart Figure 2 of your proposed staffing at a role level (e.g., desktop technician, service desk agent), showing reporting relationships to provide the services described in the RFP, including Prime and Subcontractors, starting from Account Executive and broken down into Service Frameworks.

Figure 2. Functional Organizational Chart



2.3.3 Centers of Excellence

2.3.3. The County recognizes that Offerors have centers of excellence situated in various locations around the U.S., and would like to take advantage of the best resources the Offerors have for the best price. It also recognizes that local presence matters for a number of the Services in the RFP, when face-to-face contact and on-the-ground operational capability are important, e.g., end-user, network, and applications services. This may require a balanced set of resources from a geographic perspective, including Prime and/or Subcontractor resources in the County of San Diego capable of providing the Services the County seeks via this RFP.

Provide a description, and underlying rationale, of the geographic deployment of resources at a role level (including both Prime and Subcontractor resources) to deliver the Services in your proposal response, broken down into Service Frameworks and facilities/locations, and noting specifically the percentage of local resources in San Diego County.

The HPES team will provide services from mainly five (5) locations: the County of San Diego; Pontiac, Michigan; Tulsa, Oklahoma, Colorado Springs, Colorado, and El Paso, Texas, with a few individual support personnel at various sites within the United States (individual who work from home). These sites will house staff, equipment, and services needed to respond to inquiries over the telephone and by fax, email, and web-based media including web forms. We will provide support 24x7x365, operating

seamlessly as one integrated organization. Table 2 lists the percentages of services provided from each location.

Table 2. Service Frameworks

LOCATION	SERVICE DESK SERVICES	END-USER SERVICES	NETWORK SERVICES	DATA CENTER SERVICES	APPLICATION SERVICES
County of San Diego	20%	100%	80%	10%	75%
Pontiac, MI	80%			5%	5%
El Paso, TX					10%
Tulsa, OK			10%	65%	
Colorado Springs, CO				5%	
Other resources			10%	15%	10%

2.3.4 Proposed Key Personnel

2.3.4. Name the proposed Key Personnel, and other significant resources (including both Prime and Subcontractor resources), along with their contact information (telephone number and e-mail address), Prime or Subcontractor company name, qualifications, experience, and the level and extent of their expected involvement in providing the Services outlined in this RFP.

HPES has had the privilege of supporting the County's mission for its residents, businesses, and visitors through the IT and Telecommunications program since 2006—as the prime contractor since 2011, along with our teammate AT&T. We do not take for granted the County's trust in us: our position has been and will continue to be that we have to earn the opportunity to do business with the County each and every day. We take great pride and satisfaction in the County achieving its mission of providing superior services to its citizens more than just the success of IT in our partnership.

We present several key points and benefits relative to what we can offer the County as follows and as reflected throughout our response:

Table 3. Key Personnel

KEY PERSON	TITLE / PHONE / EMAIL / PRIME / SUBCONTRACTOR	YEARS SUPPORTING THE COUNTY	DEDICATED RESOURCE	RESIDENT OF COUNTY OF SAN DIEGO
Cathy Varner	Account Executive / (P) 858 674 8600 / (E) cathy.varner@hpe.com / Prime	10	✓	✓
Laura Floyd	Deputy Account Executive / (P) 703 926 4665 / (E) laura.floyd@hpe.com / Prime	3	✓	✓
Grant Morgan	Program Executive / (P) 858 886 1100 / (E) grant.morgan@att.com / Subcontractor	10	✓	✓

KEY PERSON	TITLE / PHONE / EMAIL / PRIME / SUBCONTRACTOR	YEARS SUPPORTING THE COUNTY	DEDICATED RESOURCE	RESIDENT OF COUNTY OF SAN DIEGO
Thif Iruthayarajah	Chief Technology Architect / (P) 858 674 3597 / (E) thif.iruthayarajah@hpe.com / Prime	10	✓	✓
Marcelo Peredo	Chief Information Security Officer / (P) 703 821 0899 / (E) marcelo.y.peredo@hpe.com / Prime	1	✓	✓
Hector Vaquedano	End User Services Manager / (P) 858 674 8602 / (E) hector.vaquedano@hpe.com / Prime	10	✓	✓
Michael Boscarino	Data Center Services Manager / (P) 858 674 3520 / (E) michael.boscarino@hpe.com / Prime	5	✓	✓
Curtis Yancey	Service Desk Manager / (P) 858 674 8533 / (E) curtis.yancey@hpe.com / Prime	2	✓	✓
Max Pinna	Contracts Manager / (P) 858 674 3504 / (E) max.pinna@hpe.com / Prime	7	✓	✓
Jeff Williams	Network Services Manager / (P) 858 674 8593 / (E) jeff.williams@hpe.com / Prime	2	✓	✓
Mark Roehr	Applications Development Services Manager / (P) 650 258 9238 / (E) mark.roehr@hpe.com / Prime	1	✓	✓
Mark Morin	Cross Functional Services Manager / (P) 858 674 8505 / (E) mark.morin@hpe.com / Prime	4	✓	✓
Frank Krone	CSG Service Delivery Manager / (P) 619 757 3729 / (E) frank.krone@hpe.com / Prime	16	✓	✓
Albert Hatcher	PSG Service Delivery Manager / (P) 858 674 8626 / (E) albert.hatcher@hpe.com / Prime	10	✓	✓
Sandra Messina	HHSA Service Delivery Manager / (P) 858 674 8686 / (E) sandra.lyn.messina@hpe.com / Prime	5	✓	✓

KEY PERSON	TITLE / PHONE / EMAIL / PRIME / SUBCONTRACTOR	YEARS SUPPORTING THE COUNTY	DEDICATED RESOURCE	RESIDENT OF COUNTY OF SAN DIEGO
Nelson Diaz	Program Management Office Manager / (P) 858 674 8502 / (E) ndiaz@hpe.com / Prime	Recent Hire	✓	✓
John Steed	FG3 Service Delivery Manager / (P) 858 731 7532 / (E) john.e.steed@hpe.com / Prime	3	✓	✓
David Pugh	LUEG Service Delivery Manager / (P) 619 338 2668 / (E) david.pugh@hpe.com / Prime	16	✓	✓
Tina Terlecki	Application Maintenance & Operations Manager / (P) 619 417 8418 / (E) tina.terlecki@hpe.com / Prime	11	✓	✓
Kathleen Barghols	Enterprise Service Delivery Manager / (P) 858 674 8603 / (E) kathleen.barghols@hpe.com / Prime	6	✓	✓
Chris Spanka	Transition Manager / (P) 404 774 107 / (E) christopher.l.spanka@hpe.com / Prime		✓	**To reside in SD during Transition**

Key Personnel Qualifications

Cathy Varner, HPES — **Located in and Supporting the County Since 2006**
Account Executive — **Overall Years of Experience: 35**

Cathy Varner, Account Executive for the County of San Diego program, has been supporting the County since 2006 and has fostered strong relationships with County Executives and with leadership of our key subcontractor, AT&T. Cathy has developed an account team culture built on the foundation questions, "What problem are we solving? How does this move the County forward?' Her philosophy that "we have to earn the opportunity to do business with the County" is reflected in the dedication and commitment of her team. Prior to supporting the County, Cathy was the Account Executive for several public sector and government clients, including City of Los Angeles Department of Human Resources, Freemont Compensation, First Health, and SSP Litronic and was the Executive Sponsor for the City of Anaheim. Cathy has been a member of the San Diego Futures Foundation since 2006 and is currently serving as Board President, having previously served as Chief Financial Officer (CFO)–Treasurer.

Laura Floyd, HPES — **Located in and Supporting the County Since 2013**
Deputy Account Executive — **Overall Years of Experience: 30**

Laura Floyd is currently serving as the Chief Operations Officer (COO) and Deputy Account Executive for the County of San Diego program. Prior to her current role, she served as an engagement executive and consultant for key accounts and pursuits in HP Enterprise Services' U.S. Public Sector. In that role, Laura partnered with top accounts and pursuit teams to provide leadership and strategic guidance on a

variety of major enterprise initiatives for both existing and new accounts. Laura has also served as Managing Director for the U.S. Navy and U.S. Marine Corps Service Transition Program and COO/Chief of Staff for the Enterprise Navy Program. Efforts under the Enterprise Program Office included transition, change and release management, configuration management, and all Navy core delivery. She was responsible for managing $800 million worth of annual core service offerings. Laura also served as an HP Account Executive (AE) for the Navy account, responsible for end-to-end delivery and service performance with annual revenues of $220 million.

Grant Morgan, AT&T **Supporting the County Since 2008**
Program Executive **Overall Years of Experience: 15**

Grant Morgan is an accomplished leader and business professional with more than 15 years of experience in large enterprise IT programs. He is skilled in assimilating complex technical concepts with strategic business focus to deliver cost-effective results. Grant is adept in the development and presentation of thorough program recommendations and in building trust with program stakeholders. For the past decade, Grant has been actively supporting the County as part of the information technology and communications program. He has served as a top technical escalation point for networking issues with responsibility for making real-time technical decisions that impact both customer satisfaction and fiscal performance. The County has benefited from performance improvements and cost reductions as a result of Grant's contributions. Areas Grant supports include software defined networking, mobile device management, mobility applications, unified communications, ubiquitous Wi-Fi, WAN acceleration, network access control, data loss prevention, mobile VPN, system and firewall virtualization, cloud services, and disaster recovery architecture.

Thif Iruthayarajah, HPES **Supporting the County Since 2011**
Chief Technology Architect **Overall Years of Experience: 19**

Thif Iruthayarajah has more than 19 years of experience designing and implementing multi-tier applications and system integration solutions as an Enterprise Architect, Software Engineer, and Programmer with 11+ years in the public sector. He is experienced in enterprise applications with the ability to articulate IT solutions based on enterprise strategic business and technical requirements. Thif is adept in all facets of business and the IT architecture lifecycle including strategy, governance, planning, compliance, design, development, performance, and operation/support. He maintains in-depth knowledge of project lifecycle development from initial feasibility analysis through implementation including requirements, development, testing, deployment, support, documentation and user training. He possesses outstanding application analysis, evaluation and design review skills. Notable technical domain expertise includes the following:

Servers: Windows, Solaris, HP-UX, SunOS, AIX, Linux
Software Development: C/C++, ASP.NET, C#, JAVA, WCF, IBM MQSeries, XML, XSLT, JavaScript, UML, Shell, awk, Perl
Apps/Technologies: VMware, Oracle Application Server, SQL Server 2012 AlwaysOn, Active Directory, ADFS, LDAP, SharePoint 2010/2013, CRM, Microsoft Azure/Appfabric, Akamai DNS and Site Delivery, Adobe Experience Manager, Tibco Managed File Transfer, Enterprise Content Management, F5, LoadRunner, Data Warehouse, PKI, Firewall, VPN, Encryptions, Office 365, Mobility-AirWatch, SSO, Cloud Services
Web Service Software: Apache, Tomcat, WebLogic, MS IIS, Web authoring tools
Message Queues: WebSphere MQ (formerly MQSeries), MSMQ
Database: MS-SQL, Oracle, Informix, SQL Query, PL/SQL

Marcelo Peredo, HPES **Supporting the County Since 2015**
Chief Information Security Officer **Overall Years of Experience: 25**

Marcelo Peredo has more than 25 years of experience in software engineering, information security, and program management. He currently supports the County of San Diego as the Chief Information Security Officer (CISO). Prior to this engagement with the County, he worked at the Federal Bureau of Investigation (FBI) as a Program Manager providing Information System Security Officer (ISSO) support to field offices across the country. He also worked at the United States Secret Service (USSS) as the Project Manager for the Information Systems Security Officer (ISSO) support team under the CISO where he won the ISSO of the Year award. Marcelo has also served as DHS FISMA Inventory Management System team lead at the Department of Homeland Security (DHS) under the Office of the Chief Information Officer (OCIO). He was responsible for improving existing processes and defining new ones as well as implementing innovative support technologies to manage the DHS-IT inventory more efficiently. His certifications include the following:

- Certified Chief Information Security Officer (C|CISO), EC-Council
- Project Management Professional (PMP), Project Management Institute (PMI)
- Certified Information Systems Security Professional (CISSP), International Systems Security Certification Consortium (ISC)^2
- Certified Secure Software Lifecycle Professional (CSSLP), ISC^2
- Certified Information Security Auditor (CISA), Information Systems and Control Association (ISACA)
- Certified Risk and Information System Control (CRISC), ISACA
- Committee on National Security Systems (CNSS), Information Systems Security Professional (CNSS/NSA 4011)
- Senior Systems Manager (CNSS/NSA 4012)

Hector Vaquedano, HPES **Supporting the County Since 2006**
End User Services Manager **Overall Years of Experience: 35**

Hector Vaquedano has more than 35 years of experience and achievements managing data processing operations and personnel. Currently he is the Data Center Operations Manager for the County, responsible for the infrastructure services provided by the local and data center leveraged support teams as well as for server performance, availability, and security that includes server patching, firmware, monitoring, backup, storage, capacity management, and monthly reporting. In addition, oversees the leveraged exchange/email environment, print services, and disaster/recovery. Hector's acumen in organizational and personnel management has positively impacted all new technical operations efforts that he has led. He is committed to quality and service excellence for both existing and new technical projects. He is also able to support client-vendor relationships, development and compliance of policies and procedures, design and execution of business processes, and SLA management. Hector's professional experience also includes data center management, problem resolution, financial management, service delivery, and training and development.

Michael Boscarino, HPES **Supporting the County Since 2011**
Data Center Services Manager **Overall Years of Experience: 22**

Michael Boscarino is a seasoned professional with more than 22 years' experience in IT management, including strategic direction, budget preparation, vendor relationships, and planning and operations of IT projects. He has the ability to adapt to rapidly changing business requirements along with skills in evaluating current and future technologies for both short- and long-term initiatives. In his current position as Data Center Services Manager, Michael provides leadership and mentorship to a team of 10 system administrators supporting 225 local servers throughout the County. He coordinates and manages in-house

server builds that reduce server build time from days to hours. Other areas of responsibility while supporting the program for the County include the following:

- Creation of system architectural plans and drawings for the major local point of presence (POP) data centers
- Management of the AT&T POP for power, availability, and security access
- Support for the infrastructure team with application process expertise, bridging any gaps in communication and process

Curtis Yancey, HPES — **Supporting the County Since 2015**
Service Desk Manager — **Overall Years of Experience: 20**

Curtis Yancey has 20 years' experience in IT operations, system implementations, profit and loss (P&L) management, personnel management, and policy and procedure development and compliance. He currently manages day-to-day delivery of IT hardware and services for the County. Curtis has been responsible for recruiting, training, and managing more than 40 individuals in field desktop support and Tier II support. He has also achieved account financial and performance benchmarks. Prior to supporting the County, he served in several account management, service delivery, and program management roles for the Department of the Navy.

Jeff Williams, HPES — **Supporting the County Since 2014**
Network Services Manager — **Overall Years of Experience: 20**

Jeff Williams has 20 years of professional IT experience in information systems, operations, and strategic initiatives. He is able to crosswalk between business and technology operations that result in cost-effective and innovative solutions. Currently, he manages the AT&T network tower and related finances (approximately $35 million annually) for the County. His responsibilities include monthly billing processing for the network tower, county billing dispute resolution, and billing issue mitigation. He generates the monthly, quarterly, and annual financial projections for AT&T-related projects and services and acts as the account liaison between HPES and AT&T for County network and telecommunications activities. Jeff also manages vendor-related issues, project/outage communications, and HPES/AT&T project coordination as well as other County-related work requests and approvals. In addition, Jeff oversees network devices for the County within the HPE data centers in Tulsa, Oklahoma, and Plano, Texas, including 300 County sites and two local Point of Presence (POP) locations. He manages the team of HPES network engineers supporting the Tulsa/Plano data centers and associated network devices.

Mark Roehr, HPES — **Supporting the County Since 2015**
Applications Development Services Manager — **Overall Years of Experience: 22**

Mark Roehr is responsible for end-to-end development and solution delivery for the County, providing operational and strategic leadership for the Applications team. His responsibilities include portfolio management, shared development, database administration, application testing, and management of the applications delivery teams supporting each of the five County groups and the enterprise. Mark manages customer experience with the County to make certain that the development and delivery teams continuously meet or exceed resources, requirements, client expectations, and service levels. He has held a number of positions at HPES including Applications Manager for the Content and Digital Asset Management team and Chief Enterprise Architect responsible for the overall strategic and architectural leadership for the $10B+ Commercial Enterprise business unit. Prior to joining HPES, Mark served at NCR as the Service Delivery IT Manager responsible for development, test, and configuration management of NCR's worldwide customer services systems. Based on his experience, he has enabled the County to meet business objectives and has driven growth through close collaboration with the County, leading to innovative and effective solutions.

Mark Morin, HPES **Supporting the County Since 2012**
Cross Functional Services Manager **Overall Years of Experience: 32**

Mark Morin is an accomplished professional with more than 32 years' experience in the management of IT outsourcing and professional services projects. He has a consistent track record of managing successful teams and driving successful outsourcer/client financial outcomes that exceed client expectations. Most of Mark's career has been in client-facing roles and in leading teams with a direct impact on client satisfaction and outsourcer profitability. For the County of San Diego, Mark manages a team responsible for contract and asset management, procurement, billing and invoicing, and third-party contracts. He is a critical member of the core HPES leadership team for the County. He manages contracts for end-user computing devices, data center services, LAN/WAN/voice services, and application services for the County.

Max Pinna, HPES **Supporting the County Since 2009**
Contracts Manager **Overall Years of Experience: 23**

Max Pinna has over 23 years of legal experience. He earned his Masters of Law from the University of San Diego School Of Law. He currently acts as the Contracts Manager to the County for the IT Outsourcing Services Agreement overseeing contacting and subcontracting activities. He is the primary interface with the County for all contractual matters related to the IT Outsourcing Services Agreement. He serves as a member of the HPES executive team supporting the County where he collaborates with the HPES Account Executive and account team regarding strategic business and financial decisions.

Frank Krone, HPES **Supporting the County Since 2011**
CSG Service Delivery Manager **Overall Years of Experience: 18**

For almost two decades, Frank Krone has provided continual onsite technical and incident management services to the County. The diverse scope of his responsibility includes management of day-to-day administration and support functions to provide optimal business operations. He is also responsible for the coordination and support of technical staff in resolving priority incidents, producing trending and analytical data reports, leading weekly County Service Operations meetings, and providing daily problem management as well as root cause analysis peer review meetings. Frank serves as a key point of communication to multiple frameworks and as the liaison between the County and HPES. Certifications held by him include Information Technology Infrastructure Library (ITIL) Foundation v3 and Microsoft Certified Solutions Expert (MCSE).

Albert Hatcher, HPES **Supporting the County Since 2002**
PSG Service Delivery Manager **Overall Years of Experience: 18**

Albert Hatcher has been serving the County for more than a decade in various operations and service delivery roles in which he manages internal processes and procedures to provide the County with quality IT solutions and issue management leadership. As part of his overall responsibilities, he manages the data center, local work activities, and changes that impact the County including break/fix efforts, maintenance tasks, new projects, issue escalations, help desk maintenance, and scheduling for system maintenance. He has extensive expertise in problem management with issues requiring extended forensics and troubleshooting. Albert coordinates issue management teams that resolve conflicts and manage performance while supporting County and HPES policy for the program. He has been the County business unit's single point of contact for all operational issues and manages the day-to-day matters related to service operations including service issues and escalations. As part of his role, he works to identify opportunities for service improvement to the County. In addition, he is responsible for keeping the County informed of help desk maintenance and scheduling for system maintenance.

Sandra Messina, HPES **Supporting the County Since 2015**
HHSA Service Delivery Manager **Overall Years of Experience: 22**

Over the past two decades, Sandra Messina has supported the County on a wide range of service delivery activities. Currently, she acts as the Delivery Services and Problem Management Manager, responsible for driving severity incidents of delivery computing services to County departments according to Minimum Acceptable Service Levels (MASLs). As part of her role, she works with and across all County team towers that include applications, web services, desktops, network, telecom, server, storage, backup, security, mainframe, program management office (PMO), print and mail, and so forth. Sandra serves as the focal point of communication between HPES and the County related to high-touch incidents and problem management; she provides support for difficult customer issues and high-profile end users within the County. As part of her current responsibilities, she is charged with the facilitation of root cause analysis (RCA) activities for identified problems/incidents and making certain that corrective actions are executed according to RCA recommendations.

Nelson Diaz, HPES **Supporting the County Since 2016**
Project Management Office Manager **Overall Years of Experience: 25**

Nelson Diaz has 20 years of project and program management experience for several Fortune 500 companies as well as public sector customers. He has continued to maintain his Project Management Professional (PMP) certification over the past 12 years and was an active volunteer with the Washington, DC, Project Management Institute (PMI) chapter. His expertise includes strategic planning, controls/governance, forecasting, multimillion-dollar budget administration, and team leadership. He has experience setting up and running Project Management Offices (PMO) for customers with portfolios containing large, complex projects. Nelson is a skilled leader of teams of program/project managers, systems analysts, and consultants over a broad scope of enterprise-level projects from conception through service delivery. His results-oriented style proactively provides solutions that streamline business processes and fosters environments where team members are encouraged to promote creative/innovative solutions. Nelson's development experience encompasses the use of Agile, Ascendant, Rapid Application Development (RAD), Rational Unified Process (RUP), Scrum, and Unified Modeling Language (UML) methodologies. His results-oriented style proactively provides solutions that streamline business processes, and he fosters environments where team members are encouraged to promote creative/innovative solutions.

John Steed, HPES **Supporting the County Since 2013**
FG3 Service Delivery Manager **Overall Years of Experience: 13**

John Steed is a highly experienced and diverse professional with 13 years' experience working on a wide range of IT projects in the public and private sectors. He currently acts as a functional lead managing a suite of applications and services for the County for financial, human resources, and general IT operations. His roles have included responsibility for the following:

- Treasury Tax Collection applications including the Property Tax System, Tax Sales, and Auditor
- Controller applications such as Account Payables, Purchase Order, and Auditing
- Assessor Recorder County Clerk applications
- Enterprise Resource Planning (ERP) and Human Resources (HR) applications such as onboarding, training, and benefits enrollments
- He also supports the County in an operational capacity for service delivery, project and budget management, and operations and technical problem resolution.

Prior to supporting the County of San Diego, John supported IT projects in healthcare, the life sciences, and financial sector.

David Pugh, HPES — **Supporting the County Since 2000**
LUEG Service Delivery Manager — **Overall Years of Experience: 33**

David Pugh is a skilled IT professional with more than 33 years of experience in service delivery, incident management, continual improvement, and technical support. The vast majority of his career has been focused on IT services and support specifically to the County. He is responsible for maintaining relationships between the County and delivery teams to achieve client satisfaction. Currently, David is the Site Service Delivery Manager, orchestrating delivery teams and incident response to the County. He also acts as the primary point of contact (24x7) for any major incidents experienced by the County. Prior to acting in a service delivery capacity, he was an Infrastructure Technical Lead supporting the County's Health and Human Services and Public Safety groups. David has worked in a wide array of IT functions including network/system engineering and administration, help desk supervision, end-user support, mainframe operations, communications, process engineering, SLA performance, and incident response.

Tina Terlecki, HPES — **Supporting the County Since 2001**
Application Maintenance &Operations Services Manager — **Overall Years of Experience: 25**

Tina Terlecki is a seasoned professional with more than 25 years of management and IT expertise including 9 years in application management. She has spent the last 15 years supporting the County since the inception of the program; she maintains extensive understanding of the County stakeholders and business operations. Tina supported the County in many early innovative efforts including starting the mobile development group for the County, delivering the first native mobile application for public safety, and leading one of the first Agile driven projects—for beach and water quality. In addition, she has successfully managed three of the County portfolios, with her most current effort supporting public safety. Tina is also the subject matter expert for the Application System of Record tool and has been involved with cross-functional management, for which she is able to take quick action through her deep and extensive understanding of County needs and operations.

Kathleen Barghols, HPES — **Supporting the County Since 2010**
Enterprise Service Delivery Manager — **Overall Years of Experience: 12**

Kathleen Barghols is an experienced ITIL-certified service delivery leader. Over the past 6 years, she has served in several IT service and support roles for the County. Currently, she manages and leads a team of 80 support staff in the management of infrastructure services, both physical and virtual, for the County. Her responsibilities have included outage response, issue management, and RCAs, SLA compliance, configuration management, backup and restore, data center stand-up/support, budget forecasting, and processes with associated documentation for infrastructure. Prior to moving to the County contract, Kathleen worked on the HPES Navy account, where she advanced quickly to manage a staff of 120+ individuals for Specialized Services in Operations, which consisted of software distribution at a rate of 9 million pushes per month, user/machine account management, video teleconferencing services, messaging migration, exchange services, and SLA monitoring services.

Chris Spanka, HPES — **Will be Dedicated and On-Site During Transition**
Transition Services Manager — **Overall Years of Experience: 34**

Chris Spanka is a Senior Program Manager with 34 years of IT experience. His last three programs involved leadership of large-scale transitions and transformation projects for HPES. As leader of the Transition and Transformation (T&T) team, he mentors others in transition and transformation best practices. He is a contributor to the HPE Global Transition and Transformation Methodology (TTM) and a senior member of the HPE Public Sector Transition and Transformation Practice. Chris is routinely hand selected by HPE senior leadership to lead highly complex, large-scale transitions. His experience includes the following:

- Significant expertise in the establishment of DR environments including his most recent project for CalWIN
- Significant expertise in the buildout of new data center environments as well as migration/consolidation of existing data centers including the Mid-Atlantic Data Center
- Instrumental in the success of key transition projects for CalWIN, Mount Sanai Hospital, and Defense Manpower Data Center (DMDC)
- Leader of technical teams of more than 200 people supporting complex projects/programs within mission-critical environments.

In addition to his technical acumen, Chris is a leader of Cultural Change initiatives, focusing on the people and human factors side of transition projects. He is an effective communicator in client and business team environments, helping to drive holistic change during transition periods.

Clear Lines of Communication between the Offeror's Team and the County for Timely Problem Identification, Mitigation and Resolution

Success of complex IT projects is not based simply on IT acumen—successful relationship management and stakeholder communication are critical variables that drive program success. As outlined in Section 2.15 Offeror Response to Exhibit R-Schedule 10.3 Relationship Management, HPES has proposed a robust framework for relationship management for the program. Key counterparts have been identified between the County and the HPES program team to align the right individuals across key functions and program areas.

The CTA and the Architects are two major components of our technology team. The CTA, will have overall responsibility for setting Architectural direction and strategy (with CTO), identifying emerging trends, anticipating and understanding transformative shifts in technology, developing enterprise and departmental roadmaps, and maintaining strong relationships with our leading technology partners. The CTA will then translate this information and direction to the Architects for execution.

The Architects, who will receive strategy and direction from the CTA, will be responsible for executing that strategy including adherence to methodologies, standard processes, best practices, accelerators, and standards.

While there will be a strong dotted-line relationship between the CTA and the Architects, the CTA will report to the Account Executive and the Architects will report to the Technology Office. The intent of this structure is to unencumber the CTA from the administrative burden required when one has direct reports, including HR activities and staff professional development (these activities will be the responsibility of the Tech Office).

HPES believes this structure allows the CTA to focus on strategic direction and transformation – always looking forward.

The CTA/Architect reporting structure mirrors that of CISO/Security Ops. The CISO has overall responsibility for all aspects of security (with County CISO) while Security Ops is responsible for execution of those strategies as well as day-to-day activities (prioritization of tasks, allocation of resources) and HR administration.

To further support timely, effective, and efficient communications among the right individuals on the program, a stakeholder communication matrix has been proposed in Section 2.15, Table 94. The stakeholder communication matrix has been established based on the County's organizational structure to verify that County and HPES senior leadership and operational teams are focused and informed on the needs of the County and to facilitate strong communication and collaboration to advance County business and technical objectives.

Interaction with Customer PMs

Governed by the HPES Program Management Office, HPES project managers will interact with the County in a number of ways, including the following, to communicate program and project status:

- Hold regular standing meetings with County stakeholders including County project sponsors, County Group IT Managers (GITMs), and members of the County Technology Office (CTO) to discuss project activities including project schedule, scope, risks, issues, and/or any concerns requiring escalation
- Provide program reporting regarding the project as the County requires or requests
- Conduct frequent reviews of the program risk log to proactively address perceived project risks and associated mitigations to those risks
- Coordinate cross-functional teams and communication strategies with County sponsors around issue management, and work to resolve project performance matters to the satisfaction of the County
- Work with appropriate County stakeholders to address any capacity and demand management issues in a proactive manner
- Partner with program sponsors and vendors to deliver a consistent and predictable customer experience through established program processes and methodologies for management of the program
- When process gaps and bottlenecks are identified, establish functional teams to improve processes

Using the aligned HPES/County organizational structure, we will leverage the existing touch points listed to implement a formal communication structure that engages County stakeholders early and often throughout the project lifecycle. Some examples of interactions include the following:

- Establishing communications strategies for the specific needs of the CTO and County business groups
- Developing enterprise communication procedures and templates
- Auditing program and project communications plans
- Creating PMO and project announcements
- Developing and maintaining communication vehicles such as the PMO SharePoint, public folder, and network drive space
- Publication and management of Notices of Decision
- Creating and executing communication plans for PMO initiatives
- Preparing presentation material for internal and external reporting

Active and Continuing Participation and Involvement of Senior Corporate Executives in Ensuring the Success of this Program

A major feature of our organizational structure is the direct access of HPES senior corporate leadership to senior County leadership. Mechanisms have been put into place to provide bi-directional communication between the County and HPES across all layers of the program. Our approach addresses communication to stakeholders at the project, portfolio, and enterprise levels. Communications can be facilitated via email or meeting; meetings may be face-to-face and/or teleconference and may include Virtual Room sessions to discuss matters or view presentation materials and documents.

Cathy Varner, the HPES County of San Diego Account Executive, is fully dedicated to the County to make certain that the program receives the highest level of commitment from HPES. Cathy is authorized to draw from the vast HPES corporate resources, as needed, to support the accomplishment of program goals and objectives. HPES is committed to annual meetings with the CTO which include Cathy Varner and Steve Tolbert, VP, HPES US Public Sector.

Our team mapping aligns with the County structure and increases our ability to work collaboratively and jointly as we broaden our partnership. The relationship management approach and stakeholder communication matrix identified in the following table enables communication at all levels of the program to make certain that the County has a direct point of contact for all frameworks and their

components. Additionally, HPES has established rich relationships with the County, individually and collectively, leading to open and transparent communications that enable dialogue and decisions regarding opportunities and issues.

Ongoing meetings listed in the following tables are currently held between the County and HPES to communicate program status and updates that maintain proactive lines of communication at all times. Table 4 outlines the relationship counterparts between the County and HPES roles.

Table 4. Relationship Counterparts

COUNTY OF SAN DIEGO	HPES
CIO	Vice President and Account Executive (AE)
ACIO	Deputy AE
GITMs	Deputy AE, Enterprise Service Delivery Manager, Service Delivery Managers, Applications Development Services Manager, Project Management Office Manager
CTA	CTA
Contracts Manager	Contracts Manager
Chief Information Security Officer	Chief Information Security Officer
Applications Management	Applications development services manager
Chief Data Architect	CTA
Enterprise Application Project Manager	Project Management Office Manager
Operations Managers	Service Delivery Managers

To enhance this multi-tiered framework, a complementary communication matrix has been established based on the County's organizational structure and requirements that verify the County and HPES leadership and operational teams are focused and informed on County needs. Table 5 outlines the proposed stakeholder communication matrix to facilitate strong communication and collaboration to advance County business and technical objectives.

Table 5. Proposed Stakeholder Communications Matrix

COMMUNICATION	PURPOSE/ OBJECTIVE	FREQUENCY	AUDIENCE
Executive Meeting	HPES/County alignment of objectives and program escalations	Bimonthly or as determined by the County participant	County CIO; HPES State and Local Government VP and HPES AE
Program Status and Strategy	Program management overall program health	Weekly	County CIO; HPES AE
CIO Security Briefing	Briefing to County CIO on security strategy, initiatives, and status	Monthly	County CISO;HPES CISO, and HPES Security Officer
Executive Liaison Program Meetings	One-on-one communication between HPES AE and key	Quarterly, biannually, or	County GMs, ROV, DHR, County Council, and select

COMMUNICATION	PURPOSE/ OBJECTIVE	FREQUENCY	AUDIENCE
	County stakeholders to discuss vision and strategy. Intent is to make certain HPES is prepared to respond to County requirements.	annually, as determined by the County participant	elected officials; HPES AE and/or Deputy AE
CTO Enterprise Architecture Meetings	Review enterprise architecture solution designs, annual updates to hardware and software standards for servers, and end-user compute devices, exceptions to standards via notice of decisions, vendor technology roadmaps	Weekly	County CTA, CTO IT Staff, GITMs, County agency and/or department representation; HPES CTA, HPES technology office, and other HPES leaders as needed
Enterprise Architecture Review	Review proposed architectural changes, large project designs, architectural issues	Weekly	County CTA, CTO IT staff, GITMs; HPES CTA, HPES technology office and other HPES leaders as needed
Network Architecture Meetings	Review network roadmaps and technology upgrades	Weekly	County CTA and other CTO IT staff; HPES CTA and other HPES technical leaders as needed; AT&T chief architect
Core Meeting	Preview enterprise solution designs (detailed walkthrough) and changes to standards	Weekly	County CTA, CTO IT staff, and CISO; HPES CTA, HPES CISO, and other HPES leaders as needed
Infrastructure Project Review	Provide schedule, issue, and status data for active infrastructure projects	Weekly	County CTA, GITMs, CTO IT staff; HPES CTA, HPES technology office, and other HPES leaders as needed
Platform Status Reviews	Review project for critical County application platforms	Weekly	County CTA, CTO IT staff; HPES Application Development leader and other HPES leaders as needed.
Portfolio Review	Review of high-visibility, critical projects	Monthly	County CTA, GITMs, and CTO IT Staff; HPES business analysts, HPES Deputy AE, and other HPES leaders as needed
Portfolio Steering Committees	Review portfolio and future plans	Quarterly	County GITMs; HPES Business Analysts and other HPES leaders as needed

COMMUNICATION	PURPOSE/ OBJECTIVE	FREQUENCY	AUDIENCE
ITPMO Review	Discuss processes and procedures related to project management and process improvement with CTO	Weekly	County CTO IT staff, CTA, HPES PMO and other HPES leaders as needed
Quarterly Program Review	Provide program status, accomplishments, and operational data	Quarterly	County CTO IT staff, CTA, and GITMs, HPES AE, Deputy AE, and other HPES leaders as needed
Service Delivery Operations	Mitigate/review operation changes and issues with CTO	Biweekly	County CTO IT staff, CTA;HPES Service Delivery Executive, and other HPES leaders, as needed
Service Delivery Operations Monthly	Mitigate/review operation changes and issues with CTO and GITMs	Monthly	County CTA, CTO IT staff, and GITMs; HPES service delivery executive, SDMs, and other HPES leaders as needed
County Bricks (Technology Standards)	Document past, current, and future technology standards using Gartner's Brick framework. Brick guides solutions for the County and is updated when there are specific changes to a technology item.	As needed; triggered by product, vendor, or technology changes	County CTO IT staff, CTA, GITMs; HPES CTA, HPES technology office, and other HPES leaders as needed
Voice of the Client (VOC) – Service Excellence Initiative	Includes self-assessed ratings pertaining to delivery and client satisfaction results based on client survey feedback; our objective is continual improvement of client satisfaction and retention.	Yearly	County CTO IT staff; HPES VOC Interviewer
Information Technology Improvement Needs Assessment (ITINA) Process	HPES provides support for the County enterprise IT project planning and budgeting process—prioritization, estimating, and selection for County enterprise IT initiatives	Yearly	County IT Planning Board, GITMs, CTO IT staff; HPES participants based on subject matter expertise

2.3.5 Project Staff Selection and Replacement

2.3.5. Describe your organization's customary selection and replacement procedures for the project staff that will be providing the Services as outlined in this RFP, including your organization's willingness to commit to County requests to maintain specific staffing assignments on key County systems.

HPES' process for selection of personnel to support the County contract is as follows:

- Available positions are announced to the existing team
  - If a current employee is qualified and interested, they may post for the position
- Positions are posted on HPES websites and on Smart Buy
- Interested HPES, third parties, and external candidates may apply
- Normal hiring process includes interviews by the account team to determine technical competency and fit within the account dynamic.

As relates to the County's request to maintain specific staffing assignments:

We understand the County's request regarding HPES' position on retaining specific staffing assignments on key County systems. In principle, we are in support of keeping employees consistently engaged throughout a project's life cycle. In practice, this cannot always be accomplished.

The three primary reasons for employee or contractor replacement are: 1) an employee requests to move to another position within HPES; 2) an unexpected event occurs; and 3) contractor term limits apply.

If an employee requests to move to another position within HPES, the account team will post the position, identify a suitable replacement, notify the County (if this person was County-facing), and develop a cross-training plan so that the new team member is ready to assume the duties on the outgoing employee, making for a smooth transition. Typically an employee should remain in his/her position for a minimum of 2 years before applying for other positions. To apply for open positions prior to the minimum time requirement, approval of the employee's current manager is required.

If an employee leaves unexpectedly, the account team will immediately assign a temporary backfill to review in-flight projects and minimize disruption to the County. In parallel, the account team will post the position, identify a suitable replacement, notify the County (if this person was County-facing), and develop a training plan to make certain that the new team member has the tools necessary to perform the required functions.

HPES engages agency contractors with specific skills to augment account staff. Assignments of agency contractors from our Preferred Supplier can be made for a maximum length of engagement of 2 years. After 2 years, the contractor must leave HPE's employ for at least 100 days before they are eligible for re-engagement. If the desire is to retain the contractor in excess of 2 years, HPE will typically offer employment to the contractor. As soon as we know that a contractor has chosen not to join HPES, or at a minimum of 6 months prior to the expiration date of the consulting engagement, HPE will proactively work to backfill agency contractors with sufficient time to complete effective cross-training.

HPES encourages and supports a flexible, mobile, adaptive workforce. To this end we maintain an open posting system through which eligible employees can pursue growth and career opportunities. HPES leaders are responsible for ensuring HPES has the best talent through an annual talent review process, part of HPES' Talent Management strategy. This process provides a proactive, coordinated way to review, discuss, and share talent across HPES through a consistent set of steps, including a review of the business strategy and talent implications, an assessment of direct employees across multiple competency areas, and an action plan that includes the development of a succession pipeline and ongoing reviews and feedback.

HPES identifies the correct talent for a role through:

- Proactive management of team resources to anticipate internal moves
- Continuous development of internal resources to make sure that internal talent remains first place in filling critical roles
- Career path management – each role has multiple levels so that individuals have the opportunity to rise through the ranks and move into vacant positions

- Aligned and focused Preferred Supplier List of external agencies with whom we develop strong relationships and who understand our business should we need to seeks resources externally.

HPES recognizes that retention of resources is essential. Employees engaged in their work, satisfied with their environment, and focused on personal development prevent cost and productivity losses associated with employee-initiated attrition. We work relentlessly to see that we have the world's most competitive, committed, and innovative workforce.

2.4 Service Framework Executive Overview

2.4. Format and Questions for Responses Regarding each Service Framework in Exhibit H-Schedule 4.3 Operational Services

Each of our responses—within the County service framework—provides a concise overview to support our detailed responses to each section and subsection of that respective framework. The responses within each section demonstrate our expertise both as an IT leader in the marketplace and as a trusted service provider to the County of San Diego.

Our in-depth knowledge of the County's IT program and business operations affords us the ability to provide proven expertise in all task areas including areas where the County can gain benefit from high-performance service delivery, ongoing operational excellence, and structured approaches for continual improvement and innovation. Our ability and commitment to service excellence for the County is clearly reflected in the most recent 2015 independent Gartner *IT Services Satisfaction Survey of San Diego County Employees,* where HPES, with the County Technology Office (CTO), achieved *Best in Class* (4.2 rating).

By continuing with HPES, the County will retain an existing, successful partnership with a proven industry leader who maintains a complete service portfolio that meets and exceeds the County's current needs and has the commitment and passion to lead the county forward to meet their objectives. Our primary goal is to help the County maintain and expand its position as an IT leader within local government. The continuation of our partnership will provide the County with a secure, stable, and cost-effective way to meet County IT and communication needs for the present and into the future.

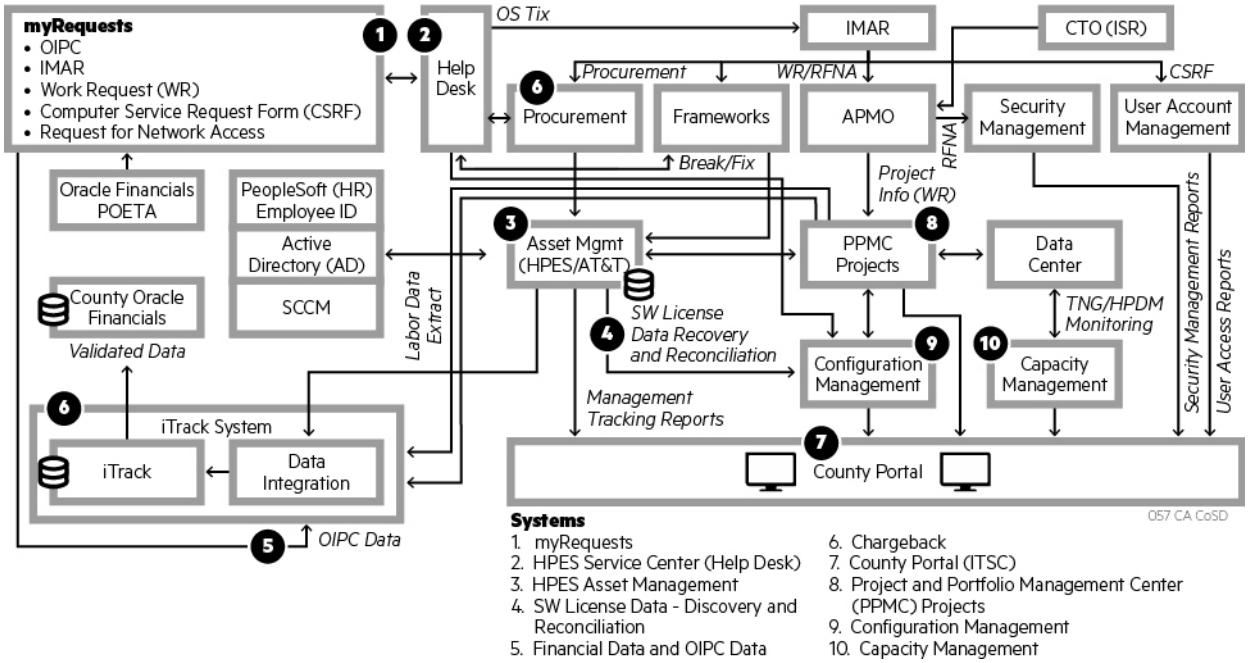
2.5 Cross-Functional Services Framework

2.5 - Cross-Functional Services Framework

Cross-Functional Services Framework Executive Overview

HPES has been providing quality, dependable, and sustainable Cross-Functional Services to the County since 2006. Our familiarity with the County's IT services and architecture, our trusted County relationships honed over time, and our commitment to the County's mission and vision uniquely qualifies HPES. Our commitment to delivering continuously improving sustainable, predictable, and reliable IT services is unparalleled in the County. HPES will reliably manage the County's IT environment through a consistent and standardized cross functional services model, illustrated in Figure 3.

Figure 3. HPES Cross-Functional Services Model



Delivering centrally managed, cross-functional uniformity of County cross-functional IT services.

Our Information Technology Infrastructure Library (ITIL)-aligned service management practices support all HPES-delivered IT services, making certain that our service delivery meets or exceeds County requirements and expectations. We will employ industry best practices, processes, and methodologies, optimally combining people and technology to fulfill the County's IT objectives. We coordinate and collaborate with County leadership, limiting or preventing misunderstanding and miscommunication through full and open transparency.

Described in great detail throughout the remainder of this section, HPES is dedicated and committed to providing integrated, inter-operating cross-functional IT services across the frameworks shown in Table 6.

Table 6. Cross-Functional IT Services

CROSS-FUNCTIONAL IT SERVICES	
• Contract and Acquisition Management • Integrated Asset Management	• Change Management • Release Management

CROSS-FUNCTIONAL IT SERVICES

• Billing Management • Security Management • Service Delivery Management (SDM) • Architecture • Project Management • Integration and Testing • Incident Management • Problem Management	• Configuration Management • Capacity Planning and Performance Management • Disaster Recovery Management • Identity Access Management • Reporting Management • Domain Name Management • Business Analyst

The Cross-Functional Services Framework serves as the primary integration of the County organization. This enterprise-wide solution encompasses HPES' policies, practices, procedures, and standards. We are excited to continue and improve our cross-functional services and build upon our organizations relationships. We understand that traditional IT services and management approaches are evolving—migrating from service towers to managed, interoperating enterprise services. Cross-Functional Services serves as the focal point to make certain that the County keeps pace with this evolution, delivering a consistent, secure IT service delivery model blended with the right combination of automation and virtualization. We share a rich history with the County, with several recent Cross-Functional Services achievements. These include the following:

- Implementation of Project and Portfolio Management Center (PPMC)
- Implementation of an improved billing chargeback system (iTrack)
- Capacity planning and performance management with zero "Red" conditions
- Development of a robust and predictable capacity plan
- Virtualization of approximately 70% County servers
- Deployment of improved testing tools like Cascade

HPES has been privileged to support the County's Cross-Functional Services for 10 years—the last 5 years as the prime contractor, along with our teammate AT&T. We do not take the County's trust in us for granted, as our position has been and will be that HPES has to earn the opportunity to do business with the County.

HPES offers several unique themes and salient characteristics relative to the County and in support of Cross-Functional Services. These features, and their benefits to the County, include the following:

- Understanding County Business, Mission and Vision
- Delivering on Reliability, Predictability, Sustainability
- Collaborating with the County on Innovation/Technology Leadership
- Providing Dedicated and Committed Personnel

HPES will provide low-risk and high-value Cross-Functional Services to the County. We plan to leverage the existing cross-functional framework with key improvements

As the world leader in IT services with a long history of creating innovative technical solutions to solve our client's real-world business challenges, HPES is in the best position to satisfy the County's requirements quickly and cost effectively. We understand what you need, and we are committed to bringing the full resources of HPES to deliver your vision for the future. HPES brings the following solid commitments to the County:

- **Key Delivery Leaders**
- **"Win/Win" Partnership Focus**: "Skin in the game" goes beyond just our delivery leaders. With a partnership this important, we are betting our reputation on the success of this program and this

relationship, and failure is not an option. Simply put, our commitment to you is that we will act as a true partner. Our actions will be guided first by what is right for your business, by our long-term relationship, and by our mutual success. We will be transparent in our pricing and in our actions, aggressively seeking ways to reduce costs and improve service.

We thank you for the opportunity to take this journey with you, and we look forward to furthering a successful relationship.

2.5.1 Contract and Acquisition Management (Sched 4.3, Section 2.3)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Solution: The HP Enterprise Services, LLC (HPES), solution includes an experienced, full-time contracts manager to serve as the single point of contact for the County on all contractual matters, including subcontracts and third-party vendor relationships. Responsibilities will encompass all contractual issues between HPES and the County, including contract interpretation, work requests, estimates and pricing discussions, and contract changes and disputes. HPES believes that contract management is an ongoing process that makes certain the County receives the expected IT and telecommunications services.

The contracts manager will establish contractor oversight responsibility and provide recurring status reports to the County contracts manager on contractual matters and will work with County counterparts to respond to unscheduled requests for information. In addition, the contracts manager will interact with subcontractors and vendors to audit and verify the timely provision of the requested services. The keys to successful contract management are an unambiguous and mutual understanding of the contract and a good business relationship. The performance standards must be articulated in the contract so that HPES and the County completely understand the standards and process for meeting each standard.

Our contract management activities will begin during the contract development process to build performance evaluative criteria into the contract. These criteria will assist the contracts manager in determining compliance with contract terms and conditions. Contract compliance depends on using the right combination of skills in conjunction with a proven contract administration methodology. Our goal is to establish project expectations collaboratively and to create a successful team based on individual accountability.

Rationale: HPES' contract and acquisition management processes are based on 5 years of experience providing County-attentive contractual services and proactive support—together with timely acquisitions at fair and reasonable prices to the County. In particular, our acquisition management system is based on processes developed by HPES' Global Procurement Organization and refined to adhere to County procurement processes.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The HPES contracts manager will oversee the delivery of the contract management services. The contracts manager is knowledgeable about the County's business and services. A subcontracts manager, procurement specialists, and HPES' Global Procurement organization will provide acquisition management. The contracts manager (Max Pinna) will be co-located in the County Technology Office, with a satellite office in Rancho Bernardo.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The methodology and processes that we use are developed by HPES' Global Procurement organization, and we develop them in conjunction and in compliance with the County procurement policies. Our

methodology includes performance-based management and includes periodic assessments of HPES' key performance indicators (KPIs). An integral component of our quality assurance management program, we continually assess these indicators to identify negative trend lines. We conduct root cause analysis, where necessary, and take appropriate remediation steps to improve the KPIs and positively influence performance trends—thereby facilitating year-to-year continuous improvement.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES' automated tools include the following:

- Aries/Aldea – Global procurement request and tracking tool
- RevGen – Procurement vendor catalog, request, and approval and PO generation tool
- County PR Log – Purchase Request tracking log.

- Qualifications and Experience – Background and experience in comparable environments

HPES uses a standard framework for contract and acquisition management procedures and for all of our outsourcing accounts, tailored to specific customer requirements. We have been providing outstanding contract and acquisition management support for the County since 2011. All HPES personnel are highly qualified with an extensive knowledge of County policies acquired over several years of *hands-on* County experience.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.1.1. Describe your organization's proposed approach to adhere to County procurement policies and procedures when engaging, selecting, and contracting with Third-Parties, including ensuring pricing is fair and reasonable.

HPES has a Global Procurement organization that is responsible for making certain that all procurements corporate-wide are performed in accordance with all Federal, state, and local laws and policies and that goods and services are purchased at fair and reasonable prices. Our approach to County procurement policies and procedures adherence is based on intimate County familiarity and established and trusted relationships—collaboratively operating in a full and transparent manner. Our procurement team maintains active and historical records of trusted and vetted third-party vendors from whom we solicit proposals and/or quotations for County goods and services. Additionally, we verify that goods and services provided were delivered in accordance with contract requirements and County expectations. Moreover, our sourcing and procurement team flows down all relevant terms and conditions to third parties to verify that all of the County's requirements are met.

2.5.1.2. Describe your proposed approach for conducting market scans to purchase Assets from Third-Parties.

The HPES procurement team submits requests for quotations (RFQs) to a subset of vendors identified by Global Procurement as best-in-class providers in their database-based Dunn and Bradstreet (D&B) ratings and other factors. We continually update this database of vendors to provide a large pool of vendors who offer competitively priced goods and services. HPES uses the County 317 – Vendor and Product Assessment Process for vendor and product assessment projects requests. Additionally, HPES' account subject matter experts (SMEs) assist in market scans by attending conferences and staying abreast of the latest technologies and products and making our procurement team aware of them. Our procurement specialists work closely with County personnel to make certain that we capture and understand their needs. We routinely follow up with them to verify their ongoing satisfaction.

2.5.1.3. Describe your proposed approach to manage, maintain and publish the Optional Item Catalog (OIPC). In your response, include a description of ways your organization will ensure fair and reasonable pricing for items in the OIPC, and a description of your proposed process for acquisition of items from the OIPC by End-Users.

HPES recognizes the importance of providing and maintaining a current, well-researched, fair-price-adjudicated Optional Item Catalog (OIC). Utilization of the OIC in the County's procurement process helps streamline the overall process—thereby enabling the on-time delivery of goods and services while minimizing on premise inventories.

The HPES desktop catalog manager is responsible for managing, maintaining, and publishing the OIC. We publish and manage the OIC via the HPES Service Portal.

HPES issues quarterly requests for quotation (RFQs) for the entire hardware catalog to multiple top-tier suppliers. We publish the lowest price obtained for each item in the OIC. If an item is not available during the 3-month period from the low-price vendor then we notify the County and request permission to purchase at the current price.

End users place acquisition requests through the Service Portal for acquisition of items from the OIC.

2.5.1.4. Describe relationships and existing agreements your organization has with Third-Party developers of government and commercial software products, and how these can be leveraged and accessed by the County.

HPES has negotiated master service agreements and strategic alliances with a number of IT and enterprise solution vendors, such as Oracle, EMC, Microsoft, Palo Alto, and so forth. In addition to favorably negotiated rates, terms, and conditions, HPES enjoys trusted working relationships providing reach-forward and reachback on demand technical support. HPES contracts with third-party developers on behalf of the County to use HPES' volume discounts, terms, and conditions.

2.5.1.5. Describe your proposed process for managing the County's Desktop Applications Directory (DAD). In your response, include the processes your organization proposes to implement to help maintain existing DAD limits.

After the review team approves the addition to the OIC Catalog for new Desktop Applications Directory (DAD) software then the HPES desktop catalog manager starts the process of adding the software to the OIC Catalog (updates to Service Portal OIC Catalog are posted on the 20th of each month). This includes purchasing software, verifying County-owned software, and transferring software requests to Desktop Engineering. After this is complete and the software is posted to the OIC, the HPES desktop catalog manager takes the licensing documentation and inputs the data into the Peregrine Asset Center database as new DAD entry(ies) updating the Asset Management Database. To manage the DAD item volume HPES will periodically produce and review with the County a report showing the last order date of all DAD items, as well as the number of instances installed. We remove items from the DAD that are no longer being ordered to remain within the DAD limits.

2.5.1.6. Describe the different hand off and touch points that will be managed to be seamless to the County End-User requesting the Service (e.g., Contract Management Services, Applications M&O Services, Applications Development Services, Service Desk Services, Network Services)

HPES, in cooperation with County stakeholders, has implemented policies, procedures, and best practices to enable the seamless provision of IT services as projects or service requests transition from point to point through instantiation or implementation.

When the customer requests a project then he or she fills out a form with the required fields and a Statement of Work (SOW) describing what he or she is trying to accomplish. After the work request form is finished and approved by the County then the request is sent to HPES as a request for a Budgetary Estimate (BE). HPES' project manager (PM) has 5 business days to contact the County requestor to provide a BE or negotiate a delivery date for the BE. The HPES PM and technical team prepare the BE with scope, requirements, assumptions, and a cost estimate for the requested work. Once approved the project proceeds to the scope execution phase. Changes in scope will be evaluated within the change management review and approval process. After the scope is completed then the project is formally closed down. The HPES PM prepares a Project Closure Agreement (PCA), and the HPES project support office (PSO) sends it to CTO Contracts. If not approved then the Project Closure Agreement is sent to the HPES PM for updates and then returned to CTO Contracts for approval. If approved, the project is officially closed, and the data in the PCA is legacy data for the project. These HPES and County tailored policies and best practices are continually refined to minimize end-user impact and disruption—enabling seamless implementation of the requested services.

2.5.1.7. Describe your approach to evaluating security to ensure the County is aware of the risks or issues in cloud-related services to enable the County to make an informed decision based on Contractor recommendations.

To provide adequate evaluation of risks and issues in cloud-related services, HPES follows the County Cloud Service Provider Request procedures, as well as HPES' Global Procurement organization's cloud service provider review process. The HPES Global Procurement processes include reviews of liability, data protection and security, termination rights, location of services, location of jurisdiction of services, control/visibility of subcontracting, rights to suspend service, and unilateral/provider amendments to service features. Our team is committed to developing policies, architectures, and solutions necessary to facilitate confidentiality, integrity, and availability of your data and systems. We will analyze evolving County architectural landscapes along with security and privacy controls, backup and continuity requirements, and user access and permissions. In addition, HPES will factor these and other considerations into our cloud recommendations and governance guidance for presentation to the County. We will apply the right level of logical and physical monitoring and management of County data center operations and cloud-based assets.

Our security experts are well versed in cloud selection, migration considerations, and user accessibility as well as denial of service to unauthorized or outside sources. HPES closely monitors these operations to facilitate strict security compliance and security risk mitigation.

2.5.2 Integrated Asset Management Services (Sched 4.3, Section 2.4)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES recognizes the challenge of effective and efficient management and optimum use of IT assets in the County environment. Another critical challenge is to identify asset criticality and devise a management strategy to avoid reactive maintenance—a relatively expensive proposition.

As part of our commitment to the County, HPES will demonstrate that we are good stewards of the assets we possess in the performance of this Contract and make sure that the IT environment runs smoothly and efficiently. We understand that our management of underlying assets is a reflection on the County. The following is an overview of our asset management solution, which will effectively and efficiently meet this challenge.

Solution: HPES will provide an Integrated Asset Management System (IAMS) that reduces the amount of manual intervention required to verify, check, and fulfill requests while adhering to governing policies and standards.

It is important that we answer five fundamental questions to demonstrate the scope and dimensions of effective asset management:

- What do you have?
- Where is it?
- How well is it working?
- How much does it cost?
- How well does it support your business?

IT asset management (ITAM) addresses these questions by providing processes, tools, data, and people across the entire life cycle. Risks associated with IT assets are articulated and managed because ITAM manages the legal obligations associated with vendor warranties and support commitments, entitlements, and asset disposal.

Our solution is based on an upgrade to HPE's Asset Manager from Asset Center. Asset Manager influences IT operations and decision making in the following ways:

- Aligns services to their supporting assets and contracts
- Effectively manages contracts, leases, license agreements, and warranties
- Streamlines the fulfillment of goods and service requests from the service catalog
- Effects complete asset and project audit tracking
- Proactively identifies license compliance issues
- Evaluates opportunities on license maintenance
- Re-harvests and reallocates unused software licenses.

HPE Asset Manager

HPES currently uses Asset Center, which will be upgraded to the enhanced HPE Asset Manager prior to the start of the new Contract. This upgrade will be performed as part of the current contract and will be seamless to the County and its users while providing enhanced performance.

In short, HPE's Asset Manager Application and associated HPES processes provide consistent and accurate inventory information. As demonstrated in Table 7, benefits to the County include productivity, cost control, and risk mitigation.

Table 7. Benefits Provided to the County

	PRODUCTIVITY	COST CONTROL	RISK MITIGATION
Hardware Asset Management	• Centralizes information and reporting to give the County a "single source of truth." • Organizes required data and provide reporting for compliance with privacy, security, and environmental regulations. Minimizes the risk of noncompliance with software contracts and auditing costs and potential penalties. • Improves asset repository accuracy by highlighting any unauthorized install, move, add, removal (IMAR) to assets.	• Maximizes use of existing hardware assets across the enterprise	

	PRODUCTIVITY	COST CONTROL	RISK MITIGATION
Software Asset Management	• Centralizes information and reporting to give the County a single source of truth.	• Maximizes use of existing software assets across the enterprise • Verifies the number of licenses in use and determines future licensing requirements based on business demands. • Assists in maintaining compliance with license agreements.	• Assists in detecting unauthorized software and enforces software restriction policies relating allowable software that is allowed to run in the County environment.
Hardware Logistics	• Provides reliable system integration facilitating correct configuration and staging of new and replacement devices so that employees are up and running with minimal downtime.		

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The following resources will be required to implement the HPES solution:

- IT asset manager
- IT SW asset manager
- Warehouse lead
- End-user HW asset analysts
- End-user SW asset analysts
- Server SW asset analysts.

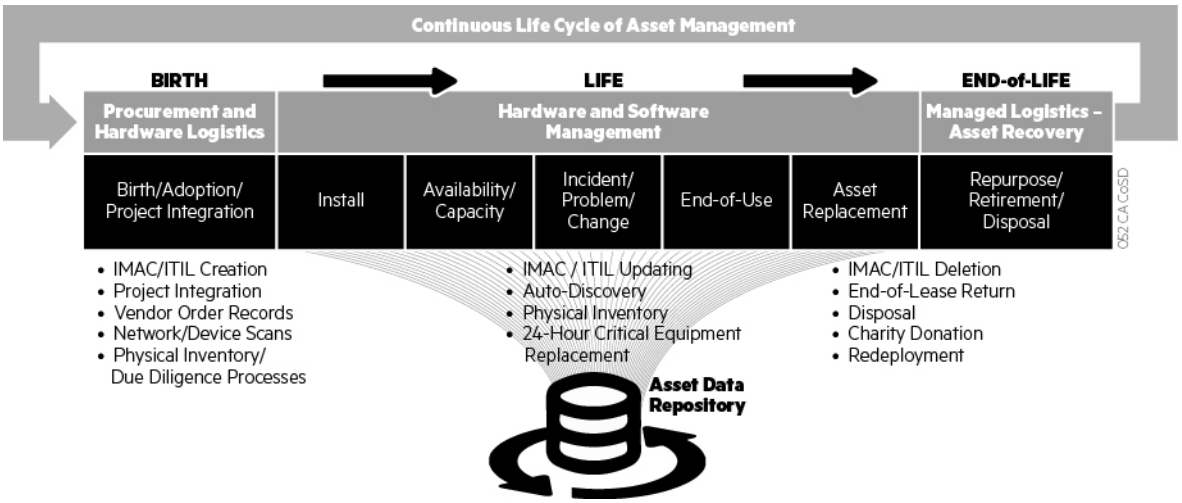
The IT asset manager and warehouse lead will operate from the HPES Rancho Bernardo facility. HPES will also leverage resources located at our Tulsa data center—the asset management team will process assets into Asset Manager and provide site support technicians based out of the Rancho Bernardo facility during IMARs, break-fix, and refresh projects for deployed desktop assets.

HPES will use a facility approach for stocking the asset inventory, employing two levels of warehouse stocking to speed delivery of equipment in support of IMARs and refresh, while mitigating both inventory and manufacturer disruption risks. County-specific inventory is held first at the HPES Rancho Bernardo facility and secondly at our partner locations.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The County benefits from an HPES asset management process that tracks all facets of IT assets, from request (procurement) to problems or changes to the asset during its useful life, to disposal (end of life). The life cycle of County asset process is depicted in Figure 4.

Figure 4. HPES Asset Life Cycle Management Process



Providing complete visibility of all County assets throughout their entire life cycle.

Hardware Asset Management

Hardware asset management comprises asset tracking and lease contracts, providing an asset repository that includes records of all hardware assets. HPES tracks, reports on, and analyzes the assets from the asset repository.

By tracking assets through the asset repository (database) using various methods and toolsets, we capture and report the asset configuration information at the device level (for example, desktop, network, and server). HPES manages the accuracy of the information through cross-checks with other systems and through process links from other services such as service desk, site support, and workplace server management services.

Table 8 identifies the County's high-level deliverables for hardware asset tracking.

Table 8. High-level Deliverables

DELIVERABLE	ACTION
Asset Repository	• Populates the asset repository with inventory records established during implementation
Asset Record Creation	• Ongoing – as new assets are procured, records are created and added to the asset repository
Asset Tracking	• Updates asset records in repository to reflect the IMAR work process while it takes place • For servers, a discovery tool remotely accesses devices and provides a channel for validating asset records • Reviews and resolves conflicts or exceptions and mediates them in the asset inventory
Reporting	• Creates standard reports documenting the current inventory • Documents inventory asset data elements specified in the table below • Documents data elements for assets that have gone through IMAR or other change processes

DELIVERABLE	ACTION
	• Records and reports on listings of noted discontinued hardware
Monthly Evaluation of Asset Accuracy	• Performs audits on approximately 10 percent of the in-scope asset records to confirm continued asset accuracy • Uses various tools to cross-check accuracy of asset data and records
Asset Exceptions Review and Resolution	• Identifies and remediates exceptions

Lease Contract Tracking

Lease contract tracking increases awareness of all applicable hardware lease agreements for the hardware assets including desktop, midrange, and mainframe platforms. This service synthesizes basic asset data with information from leasing company sources to enable tracking of all assets under lease and of those that are imminently scheduled for lease expiration.

Maintenance Contract Tracking

Through this service feature, HPES is able to compile data and aggregate it into reports detailing the general contract terms for all assets covered under warranty, including scheduled contract expirations. From this data, a monthly expiration report highlights potential renewal or replacement actions.

Maintenance contract tracking offers the following benefits:

- Provides a single database for easy access to all warranty and maintenance contracts
- Fully uses warranty and maintenance contracts and avoids expenditures for costly third-party maintenance
- Ensures ongoing warranty and maintenance coverage, where applicable.

Data collected for Warranty and Maintenance Contract Tracking and Lease Tracking is shown in Table 9.

Table 9. Data Collected

FIELD NAME	FIELD DESCRIPTION
End Date	Lease or maintenance contract end date
Expiration Date	Warranty end date
External Reference Number	External reference number (contract number)
Maintenance Contract	Number of maintenance contracts associated with an asset
Purpose	Purpose of contract
Start Date	Contract start date for lease or maintenance

Software Asset Management

Software asset management provides the tools, human resources, and processes necessary to effectively manage, control, and protect the licensed software assets throughout their life cycle. Coverage includes all in-scope desktop, midrange, and mainframe software that meets registration requirements and has the base data fields required for tracking. This includes both Desktop Applications Directory and Portfolio Applications.

HPES employs standard processes to track and maintain records for:

- Auto-discovered software found during environment scans
- Any transferable details from prior hardware asset tracking discovery
- COTS applications
- HPES-procured, -owned, and -managed COTS software, as applicable
- County-retained and HPES-managed COTS software

Software asset management includes the following services for in-scope software publishers and titles:

- Software license entitlement reporting
- Software installation reporting
- Software license and maintenance tracking
- License compliance management services

Software asset management for desktop and Portfolio Applications follows the same high-level lifecycle processes. Creation of the asset record in the IAMS occurs upon purchase and receipt of the software. The attributes of the assets and associated procurement transactions (ex. vendor, products, license metric, quantity, term, acquisition date) are populated in the system and represent the entitlement. Installation records in the IAMS are created either through automated discovery or direct entry into the IAMS. Updates to asset records are made to reflect IMARs as required.

As part of software asset management, HPES maximizes use of existing assets through re-harvesting and reallocation of existing software licenses. When there is a requirement for additional software licenses, HPES checks whether the current entitlement quantity exceeds the current quantity consumed and, if so, uses the excess licenses to fulfill the requirement. HPES also facilitates workstation/user license transfers. Licenses assigned to employees who have left the County will be reassigned to new hires; also, existing licenses may, from time to time, be reallocated to employees with a current need for that application.

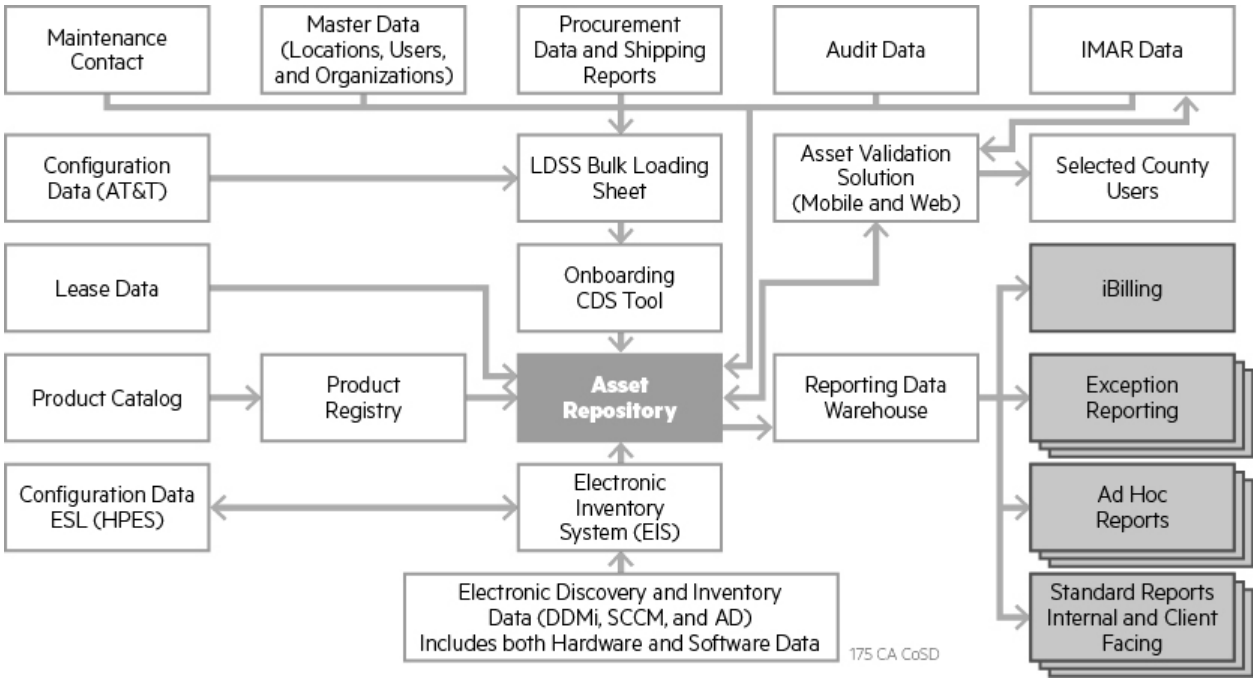
Asset Retirement/Charitable Donation

For retired personal computers, laptop computers, tablets, and associated peripheral assets that were used by the County, HPES will donate these assets to the San Diego Futures Foundation (SDFF, at no additional cost to the County). In collaboration with SDFF, HPES and the County make sure that excess IT resources are distributed to County residents most in need.

- Automated Tools – Automated systems and tools involved in proposed solution

Figure 5 depicts our IAMS. It receives data updates from the HPES configuration management database (CMDB), the AT&T CMDB, auto-discovery and inventory tools such as HPE's Discovery and Dependency Mapping Inventory (DDMI), System Center Configuration Manager (SCCM), and Active Directory) as well as bulk load updates and manual updates by asset analysts. Asset data in the IAMS will be viewable by approved County personnel using the Asset Validation System (AVS) tool, which has a link on the Service Portal.

Figure 5. HPES Integrated Asset Management System



Automated system to facilitate transparency and accuracy of all software and hardware assets.

- Qualifications and Experience – Background and experience in comparable environments

HPES has extensive experience in providing integrated asset management support, and has supported the County for the past 5 years as the prime contractor. In addition, HPES has provided comparable asset management support to numerous Federal, state, and local enterprises.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None at this time.

Answers to Specific Questions – Integrated Asset Management

2.5.2.1. Describe your proposed approach to ensure that all Assets your organization procures for the County are procured in the most cost-effective manner possible, so that the potential reacquisition of such Assets by the County in the event of a disentanglement is favorable to the County.

Our account team provides dedicated support from the HPES supply chain practice who is integrated with our team and works in partnership with us sourcing all products and services to ensure we provide the best value for the County. This resource is fully aware of our product needs, has leveraged contacts with all HPES OEM providers, and assists us procuring items in a competitive format.

HPES will employ an economic order quantity model to make sure that we are holding the minimum required inventory to be deployed to the County in the case of a disentanglement while still meeting the required refresh and IMAR commitments. This includes:

- HPES stocks a supply of desktop and laptop RU hardware units in the Rancho Bernardo warehouse against a 6-month rolling forecast based on the customer-agreed refresh plan and a buffer against IMAR estimates.

- To lessen production disruptions, we also have agreements with our value added resellers (VARs) to hold additional supplies of County-specific configured assets in their warehouses.

2.5.2.2. Describe in detail your proposed Integrated Asset Management systems and procedures, and how the County will be able to access such systems.

The HPES solution for Integrated Asset Management is based on HPES' toolset called Standard Reference Architecture (SRA), which is a proven toolset used within most large HPES accounts worldwide. Integrated Asset Management is a component within SRA. The core software application and repository used for Integrated Asset Management is Asset Manager.

Over the last year, components of SRA have already been deployed within the County of San Diego environment, including Operations Manager (HPOM), Server Automation (HPSA), Enterprise Systems Library (ESL), and Discovery and Dependency Mapping Inventory (DDMI).

Updates to the SRA toolset are made available on a regular basis. We will conduct reviews of the systems on a semi-annual/annual basis, depending on the tool, to determine whether major upgrades or replacements of systems are required to make certain that we are using the right technology to support the County's needs and remain in supported status.

The primary interfaces into Asset Manager include direct use of the client software application, the Load Data Spreadsheet (LDSS) tool for bulk loading of data from spreadsheets, and the Electronic Inventory System (EIS) for electronic discovery data.

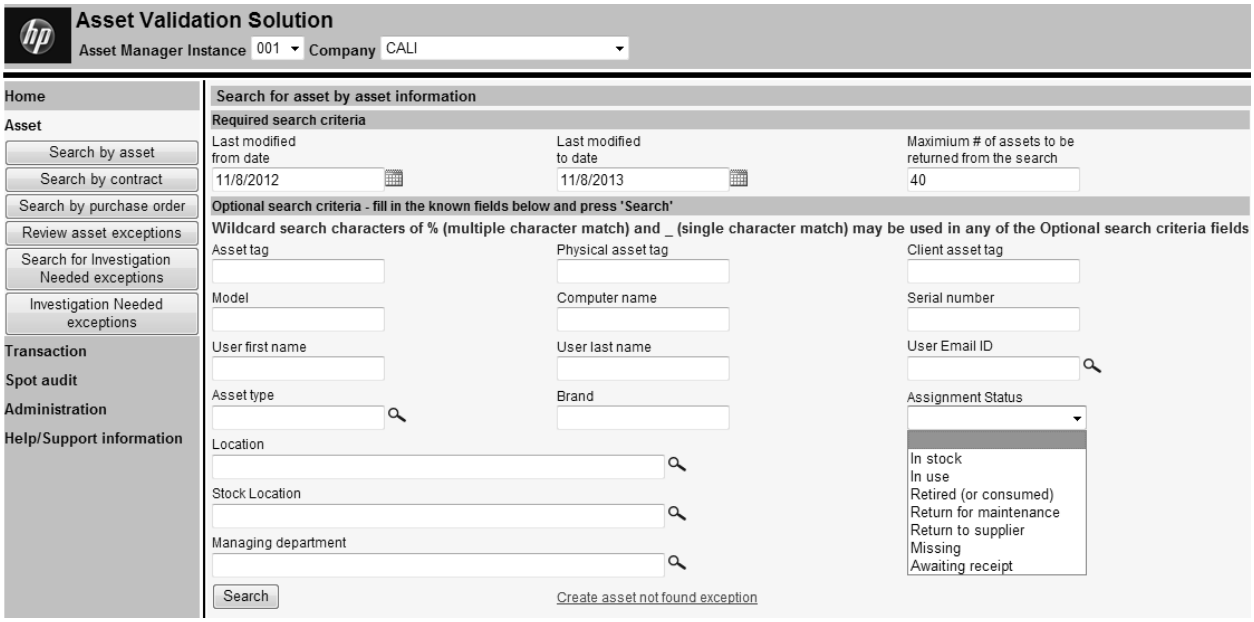
Figure 5 shows the Integrated Asset Management systems, data sources, and their integrations.

- **Configuration Data (HPES)** – ITIL-based Configuration Item (CI) data and Asset Management data are integrated. The tool used to manage CI data (ESL) is integrated with the tool used for Asset Management data (Asset Manager). Changes in CI data are passed to Asset Manager via the EIS system. EIS also handles integration of discovery tools including DDMI, SCCM, and Active Directory.
- **Configuration Data (AT&T)** – AT&T configuration data will be integrated with Asset Manager via the LDSS interface.
- **Product Catalog –** The product catalog and registry maps thousands of software and hardware names to single standard names. HPES updates this registry on a regular basis. It can also be updated with County specific applications. The product registry allows users of Asset Manager to work with a normalized set of asset names.
- **Lease Data** – For those assets that HPES leases, lease contract data is entered directly into Asset Manager's Contract Module as "lease contracts." Assets are associated with the lease contract under which they were acquired.
- **Maintenance Contracts** – The management of maintenance contracts is a standard feature of Asset Manager. Contract data is entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool.
- **Master Data –** Master data, such as County locations, is initially loaded via the LDSS bulk load tool and maintained on an ongoing basis via the client software application.
- **Procurement Data** – Tracking procurement data for assets is a standard feature of Asset Manager. Procurement data is entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool upon receipt of the assets.
- **Audit Data –** Tracking audits of assets is a standard feature of Asset Manager. Audit data is entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool.
- **IMAR Data** – Updating assets in response to IMAR changes (ex. an asset move) is performed via the client software application, LDSS bulk load too, or Asset Validation Solution (AVS), described below. AVS will allow field technicians to directly update Asset Manager in the field.

- **IBilling** – Exports of asset data from Asset Manager are imported by the IBilling system for the purposed of billing asset-based Resource Units**.**
- **Reporting** – As part of the SRA toolset, a Reporting data warehouse provides support for standard reports, ad hoc reports, and exception reporting.

HPES' IAMS, described above, will be accessible to the County. Currently, the County's iTrack chargeback system provides basic asset data in support of monthly resource unit charges based on assets. HPES is proposing to provide a subset of the County manager's direct access to asset manager data using the AVS via the Service Portal. AVS is a web user interface directly reading live asset data. A screenshot of AVS is depicted in Figure 6.

Figure 6. HPES' Asset Validation System



The AVS will be designed to give the County complete insight into its software and hardware assets.

2.5.2.3. Describe your proposed approach to ensuring ongoing management of the Asset inventory and configuration data. In particular, address how inventory data will be maintained for any system components shared with other customers.

The HPES IAMS will receive feeds from DDMI (auto-discovery for server) and SCCM and AD (desktop) and be compared to the CMDB and asset repository for accuracy. Asset records will be updated to reflect that data as necessary, and reports provided to be actioned against when an asset has not been discovered after a set period of time.

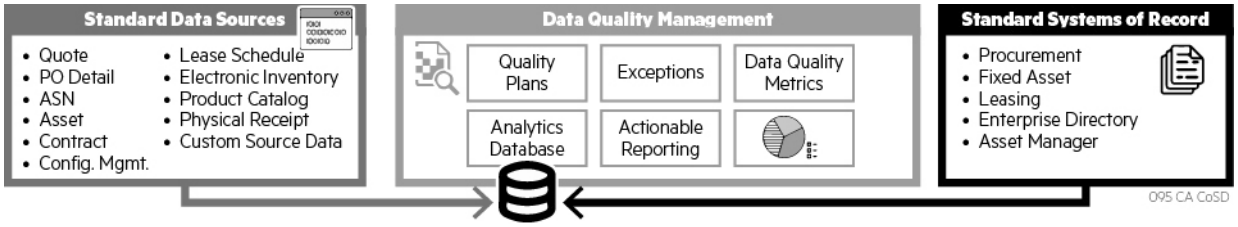
All changes to CI's are managed through our ITIL-based change management process. No changes to assets will be allowed unless previously approved.

HPES CMDB (Enterprise System List - ESL) and Asset Manager are housed in a secure, U.S-based network segment on the HPES internal network that houses only State and local Government data.

Additionally, a comprehensive review of IMAR tickets and refresh project updates is undertaken at the beginning of the billing cycle to make sure the asset data is accurately reflected in the files submitted to the iTrack system.

HPES has a data quality management process to validate the accuracy of data in our database. That process is shown in Figure 7.

Figure 7. Data Quality Management Process



Proven process to ensure the integrity of all Asset Management Data.

HPES validates asset accuracy through the following processes:

- Electronic Discovery – validate Asset Manager assets against assets discovered/active as reported in SCCM, DDMI, AD, and SEP.
- Lease Comparison – HP Financial Services asset lease database is compared to Asset Manager.
- HPES Fixed/Leased Audit – a randomly selected asset sample is validated via auto-discovery or, if required, manual inventory.
- IMAR – Support technicians validate assets when working on machines.
- Onsite Refresh Pre-Field Inspections – desktop and laptop asset data is validated one month prior to a scheduled refresh.
- HPES Data Center Asset IMACD processes – all parent assets have an affixed RFID tag, which is scanned as the asset enters or leaves the data center floor, updates are passed to ESL, which updates Asset Manager.

2.5.2.4. Describe your approach to integrate all asset repositories across the Service Frameworks.

The HPES approach to integrate all asset repositories is detailed in the automated tools section above. The details of how the system will integrate across service frameworks starts with the HPE Asset Manager asset repository containing and receiving updates to:

- Physical servers
- Virtual servers
- Storage frames
- Network appliances
- Discoverable server software
- Desktops
- Laptops
- Workstations
- Tablets
- Network printers
- Discoverable end-user asset software
- AT&T managed network devices

Updates to this data will be made via bulk loads (for example, refresh projects, move projects, new assets), nightly feeds of HPES CMDB data (ESL), AT&T data, auto-discovery and inventory data, and manual updates as requested by service manager tickets submitted to the asset management queue (for example, IMARs).

2.5.2.5. Describe integrated reporting across Assets to show useful information relating to departments, hardware, software, licenses, versions, etc.

Deployed and billable server and end-user data will be pushed to iTrack on a monthly basis. In addition, HPES will upload monthly Schedule 5 reports to the Service Portal. These include, but are not limited to:

- Report 89 – End-user status changes, deployed end-user assets, static access assets
- Report 200 – Monthly report of installed end-user software titles
- Report 17 – Monthly end-user refresh report

HPES is deploying Enterprise Services Asset Analytics (ESAA) data analysis and statistical reporting engine as part of the SRA toolset. This tool analyzes data stored in Asset Manager and generates standardized reports for analysis and action including the following:

- Asset record completeness (against pre-defined fields)
- Discoverable devices not discovered
- Discovered devices not showing in Active status
- Assets reaching end-of-life
- Devices approaching end-of-lease
- Devices updated in the last month
- Counts of tracked installed software titles versus entitlement counts

Reports are provided to the appropriate desktop or server personnel for research, corrective action, and data updates to the source systems if needed.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits

None at this time.

2.5.3 Billing Management (Sched 4.3, Section 2.5)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The County, with support from HPES, migrated to the current County chargeback application, iTrack, in January 2014. This application, combined with the HPES billing data consolidation application (IBilling), comprises the tools and associated processes for Billing Management. In February 2016, HPES migrated its IBilling application to current operating system (OS) and database technologies. Additionally, we implemented greater automation, reporting, and standardization of processing billing data feeds. HPES proposes to retain these tools and processes, while focusing on the continuous improvement achieved through collaboration with the County.

The iTrack user community, County CTO team, and HPES have identified specific opportunities for incremental improvements. As an example, managing and communicating County low org changes has been a focus area. HPES is increasing the integration between IBilling and iTrack in support of improved Low org management by enhancing IBilling to use low org data directly from iTrack for data validation. Additional enhancements that HPES plans to pursue with the County include integration with PeopleSoft HR for employee-related chargeback data and general chargeback data normalization.

We designed the current billing management systems and processes to provide accurate and timely invoices with an appropriate level of detail; generate electronic billing information to facilitate the County's chargeback activities; and support activities required to audit, validate, and substantiate billing.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES uses the following resources for our billing management services:

- **Billing Manager** – Responsible for the successful delivery of all billing management services
- **Billing Team** – Technical resources to support the IBilling application and the Framework owners responsible for providing monthly billing data and responding to billing disputes.

The billing manager will be based in the HPES Rancho Bernardo facilities.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The methodology and processes used are a combination of standard billing methodologies developed by HPES across our client accounts as well as those developed in conjunction and in compliance with the County billing and management policies. Our methodology includes performance-based management as well as periodic assessments of HPES' Key Performance Indicators (KPIs). As an integral component of our quality assurance management program, we continually assess these KPIs to identify negative trends. We conduct root-cause analyses where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, facilitating year-over-year continuous improvement.

- Automated Tools – Automated systems and tools involved in proposed solution

We use the following tools in support of billing management:

- IBilling: HPES' billing data consolidation application based on SQL Server and SQL Server Integration Services (SSIS).
- iTrack: The County's customized implementation of Nicus' M-PWR commercial off-the-shelf (COTS) chargeback application
- Billing Source Data Tools:
  - AssetManager
  - ServiceManager
  - PPMC
  - Active Directory
  - myRequests (myRequests will be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in Section 2.11 Transition Services Framework, 2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5), Special Cross Functional Project – Replacement of myRequests)
  - AppsManager
  - CSRFs
  - Service Requests

- Qualifications and Experience – Background and experience in comparable environments

HPES uses similar billing management systems for our outsourcing accounts, each tailored to meet specific client requirements. Because we have been delivering quality billing management support for the County since 2011, we bring deep familiarity with County billing management policies, procedures, and proven best practices.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.3.1. Describe your proposed approach to coordinate and reconcile detailed billings and usage on a monthly basis.

The billing team collects input data from the authoritative source systems by the 5th of each month for each framework: Application Services, Desktop Services, Network Services, Data Center, Cross Functional Services, Special Requirements, Catalog Items, and Other. During this initial data collection phase, framework owners will review both summary reports and rule-based exception reports to verify data completeness and quality.

Following collection of the framework input data, the data is aggregated in a format that can be imported into the County iTrack chargeback system by the IBilling application. IBilling applies rule-based billing logic as well as data lookup from reference systems. Additional summary, trending, and exception reporting is performed on the aggregated data.

By the 9th of each month, we review a summary invoice with the framework owners, billing team, and account management. We explain any variances and, if needed, make corrections in the billing system and rerun the processes.

After HPES management approval, we create an invoice in Excel—"Base Services Invoice"—and deliver it to the CTO and the office of Auditor and Controller (A&C) no later than the 10th of the month.

2.5.3.2. Describe the proposed interface of Contractor billing system to County iTrack, and how appropriate billing data will be transferred to the County iTrack on a timely basis.

By the 10th of each month, detailed billing data is loaded into iTrack from IBilling, the HPES billing data consolidation application, using automated Structured Query Language (SQL) scripts.

County staff process the data using iTrack and notify their staff that the data is ready for their review. Detailed telecommunication records are also loaded by the 10th of the month. All billing data, including source files, are archived for audit purposes.

2.5.3.3. Describe your proposed processes to ensure a high level of billing accuracy each month.

HPES has developed and refined billing summary, exceptions, and trend reporting based on our years of experience working with millions of records of source data each month as well as knowledge gained working with thousands of billing items within the County iTrack chargeback system. The billing team and framework owners research and address anomalies in trending and exceptions to facilitate a closed loop feedback review and continuous improvement. We have established monthly metrics to track responsiveness to County change requests; we monitor and remediate these when necessary as part of our ongoing performance-based management methodology.

In 2015-2016, HPES upgraded its billing system to provide greater automation, reporting, and standardization. This will provide a platform for enabling more rapid response to changes along with continuous improvement.

In collaboration with the County of San Diego, HPES has refined the iTrack Change Request processes. Responding to and acting on iTrack Change Request transactions is a key component providing accuracy in the overall billing process.

2.5.3.4. Describe your proposed approach to making billing corrections, and how they will be updated and corrected prior to the next billing cycle.

The Change Request process in iTrack is used to make billing corrections. Currently the County has until the 22nd of each month to create a Change Request in iTrack to dispute a charge or to request a name,

location, low org, or other change to a billing record. On the 23rd of each month, the HPES billing manager will generate a report from iTrack of all approved Change Requests for that period and will distribute it to all framework owners. The HPES billing team will investigate, correct, adjust, or explain all disputes and corrections by the next billing cycle. We will make corrections in the source systems to provide accuracy in subsequent billing periods.

Credits and adjustments for disputed charges, once validated, will appear as a credit in the next billing period.

HPES' billing manager will enter comments in iTrack stating the resolution of each dispute. We will monitored and follow up on unresolved disputes and track them through closure.

After each billing period, by the 15th of the month, the HPES billing manager will compare the Change Requests approved to the latest billing file and will follow up with framework owners on any differences to verify chargeback billing accuracy.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.4 Security Management (Sched 4.3, Section 2.6)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES' security management comprises a set of policies and procedures for systematically and quickly reacting to incidents or events that affect the County's information infrastructure, systems, and sensitive data. Our goal is to minimize risk and facilitate continuity of County IT operations by proactively preventing and limiting the impact of security breaches, whether internal or external. HPES, throughout our globally-deployed security management organization, enjoys proven success in designing, implementing, maintaining and protecting data and assets of our customers. We bring this expertise and experience to the County and will work closely with security counterparts and stakeholders to effectively and efficiently improve County information security. Our solution contemplates multiple factors that at a minimum include:

- Chief Information Security Officer (CISO)
- Risk management program (framework)
- Evaluation and recommendation for tech controls
- Security governance program/board
- Security and risk management awareness training program
- System categorization for information ownership, classification, accountability and protection
- Incident/threat management and response plan
- Security Information and Event Management (SIEM)
- Continuous improvement

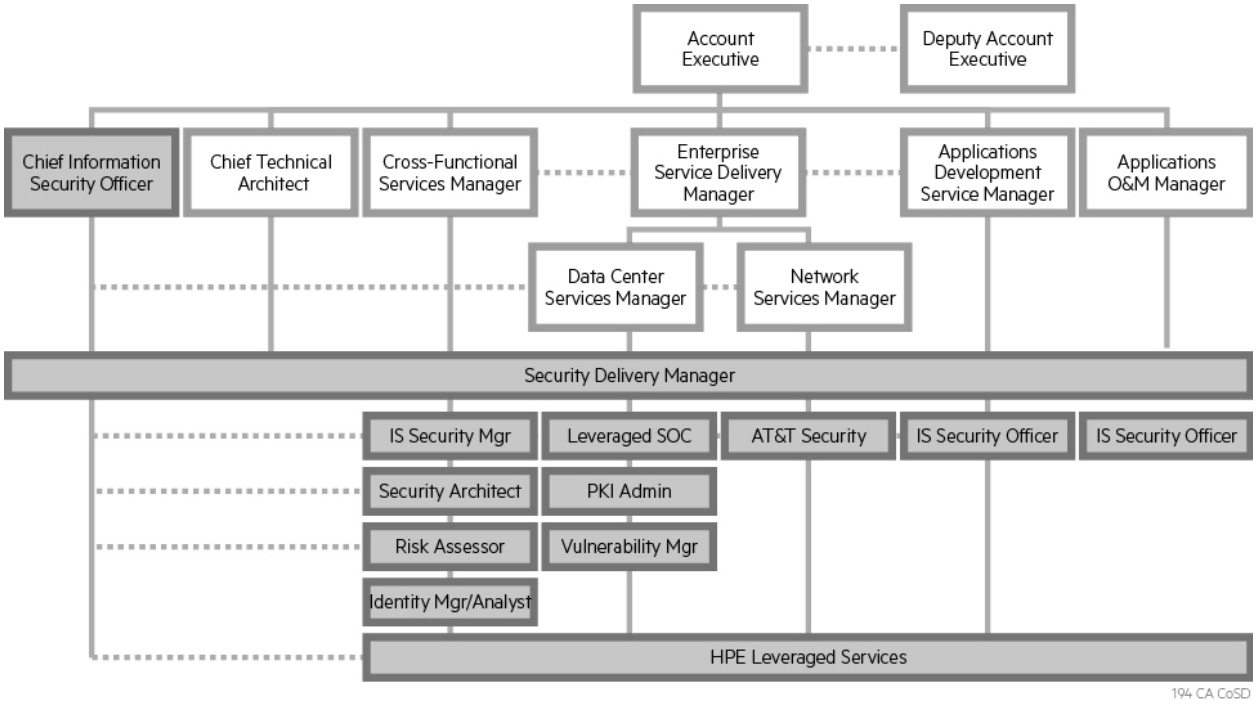
Solution: HPES' approach to security management adheres to the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) and its Special Publication 800 series, which will act as a guide for delivery and compliance for the protection of systems and providing security services to the County. Overseen by the HPES CISO, we will leverage this guidance to methodically assess systems and the organization for gaps and vulnerabilities based on the threat landscape, which may pose a level of risk to the organization. The visibility and managing of the identified risk enables the County CISO and other executives to make informed decisions that may lead to the prevention of data loss, financial loss, and most importantly the County's reputation.

A second approach, which coexists with NIST standards, is the NSA defense-in-depth model that emphasizes the use of layers and multiple defense mechanisms across the infrastructure to protect data, systems, networks, and users. In the event that one defensive measure is attacked and exploited, there are additional layers and measures to continue to protect the assets.

Additionally, HPES uses Gartner's Security Process Maturity Model to assess and report the "State of Security" and the progress of various security efforts that contribute to the overall security posture of the County. This model scores areas of security based on scale of 1 to 5 scale—the larger the number, the more mature the security aspect being modeled. Gartner provides a score for "peer" values derived from organizations with similar profiles. This maturity model is useful for comparison over time on how well the county is doing in relation to its peers. Moreover, it provides actionable intelligence for use in HPES' continuous improvement practices.

Figure 8 depicts the matrixed Security organization that works under the direction of the CISO. The CISO has overall responsibility for all aspects of security (with County CISO). In support of CISO initiatives, strategies, roadmaps, and transformation, the Security Operations Manager will be responsible for day-to-day operations and activities, which will be coordinated with the CISO for allocation of resources, prioritization of tasks, and management of leveraged resources. HPES believes that this structure allows the CISO to focus on strategic direction and transformation by having the entire team support the execution of new initiatives while maintaining and maturing existing operations—always looking forward.

Figure 8. Security Organization



The Organizational Chart depicts the Security Team led by the CISO along with the supporting team in a matrix organization.

Within the scope of the contract and in each framework, there are several security roles fulfilling each of the requirements stated in the RFP. Following are descriptions of each role and their areas of responsibility:

- IS Security Manager – Responsible for all aspects of compliance, applications security reviews, overall information systems (IS) security, data classification, NIST-based guidance, continuous monitoring of controls, and Security Awareness and Training.
- Security Architect – Responsible for security infrastructure and product roadmaps, strategic participation with other frameworks, establishment of secure zones, and infrastructure security.
- Risk Assessor – Responsible for IS risk assessments, strategic risk guidance, compliance support, vulnerability management support, and vulnerability mitigation support.
- Identity Manager/Analyst – Identity and access management, maintain federated identities, monitors and maintains automated access request workflows, user provisioning coordination, monthly IAM reports, yearly attestation process, annual update of IAM plan.
- PKI Administrator – Responsible for use case development in coordination with Security Architect, public key infrastructure (PKI) services delivery, upkeep of CPS document, manage certificate lifecycle, monthly reporting, PKI inventory, and maintenance of public key certificates.
- Vulnerability Manager – Responsible for continuous scan of the perimeter, vulnerability and risk assessment support, vulnerability mitigation, threat management plan/remediation, application scans, coordinate security operations center (SOC) activities, event log analysis and reporting, intrusion detection system/intrusion prevention system (IDS/IPS) management, data loss prevention support, incident management plan/response/handling, and forensic activities.
- Leveraged SOC – Event log monitoring, single pane of glass, unified threat management, incident response, and IDS/IPS monitoring and analysis.
- AT&T Security – Responsible for providing protection from unauthorized use, access, physical access to County hardware/software (HW/SW), firewall management, event logging, analysis, reporting, IDS/IPS in the communications infrastructure, hardware maintenance, identify and correct single point of failures, architecture and management services, roadmap maintenance for network services, incident response, data loss prevention support, web content filtering, and hardware maintenance to maximize performance.
- IS Security Officer – Responsible for overall security posture of applications, coordination with application owners, and security documentation.
- HPE Leveraged Services – Forensic services, IDS/IPS service, antivirus services, SIEM services, firewall rule implementation, and PKI support.

Rationale: HPES has successfully provided, maintained, and managed County IT systems in a secure operational manner that validates our security management solution and capabilities. Our experience and expertise with NIST 800 series, combined with our intimate familiarity with County systems and operational requirements, informs our solution and security management best practices.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The HPES security team uses multiple locations in support of the County contract. This team will work closely with the County CISO, CIO, CTO, and other IT personnel, enabling direct communication and the ability to reach out directly to the HPES team at any time.

The HPE Rancho Bernardo facility will be the center of support for our staff assigned to support the County. This facility provides centralized meeting spaces for engagements between the County contractors and HPES personnel. It also includes test environments, training room, video conferencing, and HPES executive offices.

HPE Tulsa Data Center will provide the majority of County IT infrastructure and core IT services, including web, application, DB servers, data storage, and data management.

HPE Orlando data center hosts the leveraged ArcSight SIEM solution from which the county's IT infrastructure is monitored 24x7x365.

HPE Colorado Springs Data Center will serve as the disaster recovery site for the County IT services.

HPE U.S. Public Sector (USPS) headquarters in Herndon VA will serve as the primary location for senior HPES executives and the Enterprise Security Operations Center (ESOC), a service that monitors the SIEM service.

Various other County buildings such as the County Administration Center (CAC), County Operations Center (COC), any facilities that provides meeting capabilities for the HPES security services team to conduct business.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES uses the NIST CSRC information security tools, practices, standards and guidelines to support the County. The CSRC is the primary source of information for security related standard publications that provide computer/cyber information guidelines, recommendations, and reference materials. In addition, HPES will rely on NIST Special Publication 800-53 and 800-37, focusing on the Risk Management Framework (RMF) and the County implementation. The RMF is currently in use by all Federal agencies to comply with FISMA requirements. HPES understands that the County currently does not have a Federal mandate to comply with FISMA. However, there are some systems in the law enforcement community and healthcare systems that require a proven standard to protect those Federal systems as well as systems that may have interfaces to them. HPES has been instrumental in developing a roadmap for deployment and adoption of the RMF and has also been involved in tailoring the framework implementation in a manner that is non-disruptive, and aligns and complements current policies, operations, and strategic goals. Following is a high-level description of each methodology and key processes that are relevant to the County.

Risk Management Framework – RMF will be the framework for the County's risk management program and will provide a standard to measure systems critical to the ever-changing threat landscape in today's County IT infrastructure and systems future hybrid cloud environments. Measuring security controls against an established standard enables best-case resource use and an optimal security posture in which the discovery of vulnerabilities and the time it takes to mitigate them takes as little time as practicable. By following and adhering to the RMF, HPES will be able to minimize potential security oriented exploitation and reduce the risk/impact to the County. As an industry leader of security software, we are committed to automating the testing of as many controls as possible, relying on human intervention as it is appropriate and necessary. The RMF implementation will continuously look for ways to automate and benefit from technology throughout the duration of the Contract. The essence of the RMF is its simplicity and its versatility to align and integrate with other frameworks. It employs data visualization technology using dashboards influenced by users and graphical representations to reduce the complexity and improve the accuracy of reporting. The risk-based approach to security control selection and testing will provide effective and efficient applicability to the laws and regulations that the County must follow. The steps in the RMF Model, illustrated in Figure 9 are:

- **Step 1: Categorize -** Categorize the information system for ownership, classification, accountability, impact analysis and protection; information is processed, stored, and transmitted by that system.
- **Step 2: Select -** Select an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on the County's assessment of risk and local conditions.

Figure 9. RMF Framework

Providing methodical approach to risk management.

- **Step 3: Implement -** Implement the security controls and document how the controls are deployed within the information system and environment of operation.
- **Step 4: Assess -** Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly and operating as intended, to meet the security requirements for the enterprise.
- **Step 5: Authorize -** Authorize information system operation based on the risk to the County's operations and assets, individuals, third-party vendors; the County determines acceptable risk.
- **Step 6: Monitor -** Monitor and evaluate selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate County officials such as the CISO, CIO, and CTA.

The benefit of including IT security requirements as part of the engineering and architecture of a solution is that there will be no rework to incorporate security and thus less costly, more efficient and logical that the solution will be built to withstand the protection the environment and data require. Conversely, implementing and testing controls later in the systems engineering life cycle can be costly and in some instances may even be difficult to achieve the levels of security desired for a solution. HPES will provide security early (planning), often (throughout implementation), and rarely as an add-on afterthought (except in emergency situations).

Another key advantage of the RMF is the review framework-based risks and how they integrate with other frameworks and groups within the County such as HR and Procurement. NIST Special Publication 800-53 revision 4, a security control document, provides guidance to fundamentally strengthen the information systems and the environment in which they operate. The HPES security services team will provides the requisite knowledge and understanding of each control to take advantage of the expanded set of security and privacy controls. This will facilitate integration with other frameworks and other County groups that may be considering the implementation of cloud-based solutions with other vendors. In addition to managing complexity, the HPES security team will leverage the concept of common controls and control inheritance to optimally secure each system in the environment. This will result in streamlined operations, testing, and more robust application security in already existing traditional and forthcoming cloud hybrid environments.

HPES has a proven record of successfully implementing the RMF in other organizations with similar security needs; empowering decision-making based on risk, transparency, and improving visibility. The tailored RMF roadmap will make sure that its transition and evolution is low risk, non-disruptive, adaptive, and flexible to meet County demands, as the adoption of cloud-based and hybrid solutions continue to evolve. Security and the RMF are integral to any new IT initiative and avoid the stigma of "delaying" or "preventing" IT projects from moving forward by making sure every stakeholder is informed, educated, , and understands the broader and bigger goal of building IT solutions faster and more secure where all frameworks have win-win paths forward.

The ultimate goal of having a successful governance, risk, and compliance implementation at the County is the ability to make informed risk-based decisions, possess a close-to-real-time view of risk across the enterprise, comply with all Government, state, and county regulations, and have transparency in all IT operations. HPES recognizes that this is not a snapshot-in-time goal and it is an ongoing effort to make sure that all the underlying technology, processes, procedures, as well as trained individuals, are in-place and involved in all aspects of IT security at all times.

HPES is keenly aware that third-party service providers have the capacity to introduce and create risk to enterprises due to not having jurisdiction on governance and standardization when it comes to security. HPES is constantly looking for mitigating factors that contribute to lowering risk when working with

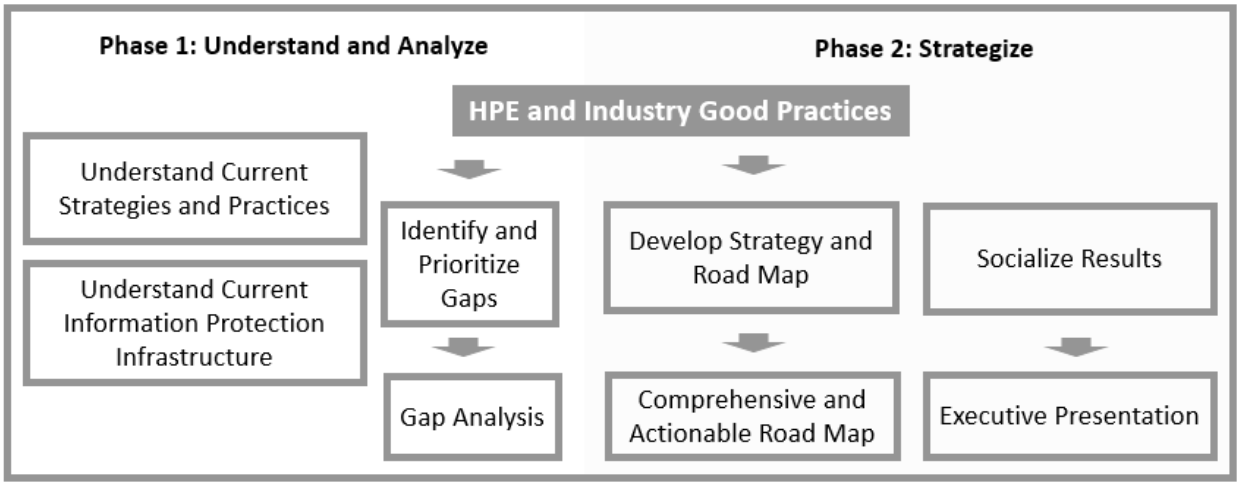
third-party vendors. As more hybrid cloud-based solutions are introduced to solve business needs, the controls surrounding third-party vendors will be rigorously tested and enhanced to minimizes risk and avoid delays. Controls designed to monitor ingress and egress of data, data flows, audit and accountability, security monitoring, and many others will be the focus of HPES when interacting with third-party vendors. A robust identity management solution as the one proposed in Section 2.5.13 will further improve the security posture by allowing the use of multifactor authentication, device authentication, and a comprehensive set of access controls based on groups and roles.

Defense-in-depth – This approach was originally conceived by the NSA as a holistic method to information security. HPES' implementation of this approach will achieve the goal of delaying the attack and buying time to detect and respond in an effort to mitigate or eliminate the consequences of a breach. Elements of defense-in-depth include antivirus, identity management, biometrics, demilitarized zones, data centric security measures, encryption for data at rest and in transit, firewalls, hashing of passwords, intrusion detection systems, logging of events for auditing, multifactor authentication, vulnerability scanning, physical security, access controls, awareness and training, virtual private networks, sandboxing, intrusion prevention systems, and others. Architecting systems appropriately is key to making sure that all available layers of defense are maximized and optimized for each system. Several of these technologies and defenses are detailed and explained in Section 2.9 as part of the data center framework. It is also important to note that each defense strategy is represented in the RMF in the form of a control or groups of controls. For example, encryption is part of the system and communication family of controls under NIST. More specifically, Control SC-13 specifies the system implementation and use of cryptography to protect data in transit, at rest, and provide digital signature nonrepudiation capabilities, among other benefits.

IT Maturity Model – HPES and the County use a Gartner IT maturity model that assesses the County's information security program and helps provide recommendations for areas of improvement based on the areas identified. It also provides recommendations, technical and non-technical, to address issues. The results will be presented to the CIO on a monthly basis or as required.

This methodology, depicted in Figure 10, consists of two phases—understand and analyze and strategize.

Figure 10. Gartner Maturity Methodology



The Gartner IT Maturity Model drives excellence through analytical and strategic best practices.

The first phase involves understanding the current state of the environment and all relevant aspects of the County's IT program such as assessing the effectiveness of controls in place and determining gaps. The

second phase consists of developing a strategy to narrow those gaps and continually update and prioritize a comprehensive security roadmap. The report is presented in a chart depicting various aspects of security that have been assessed over time.

The areas of focus include but are not limited to:

- **Governance, Organization and Personnel***:* How the County's information security function is organized and governed, and what the scope of the information security program is. How the County staff organizes its information security function, where it will get support from within, where it will be supplemented using third-party service providers, and what areas will require investment in training and hiring.
- **Policies, Standards, Procedures and Documentation:** How the County articulates and communicates its policies for information security to the business, and how these policies are supported by clearly defined standards and operational procedures. How the County stores and manages the documentation relevant to its information security environment, including as-is state, in-flight projects, assessments, audit findings, and other related materials.
- **Information Classification:** How the County classifies information and critical systems to determine appropriate information security measures based on the organization's appetite for risk.
- **IT Risk Management and Compliance:** Describes the County's risk posture, and how it assesses whether to accept, transfer, mitigate, or avoid certain risks. How the County manages its responsibilities with respect to legal, regulatory, and audit compliance.
- **Identity Management:** How identity management technologies and processes are used to create and manage identities of the various County constituents (e.g., employees, vendors, contractors, etc.)
- **Runtime Access Control:** Determines what technologies and processes are used to manage permissions and access to the County's networks and applications.
- **Software Development and Testing:** Describes how a security mind-set is integrated with software development life cycles, secure coding practices, outsourced software development, and infrastructure deployments. Describes how systematic testing of code, applications, and infrastructure components is integrated in life cycle processes.
- **Applications and Information Repositories:** How security implications relevant to applications, application development, portals, communication and collaboration platforms, file storage and transfer are reviewed.
- **Encryption:** Describes how the County uses encryption for protecting data in transit, data at rest, strong authentication, and digital signing?
- **Security Awareness and Training***:* How the County communicates the importance of information security to the business at large.
- **Change and Release Management:** How the County controls changes in their hardware, software, and supporting infrastructure while maintaining suitable and appropriate information assurance.
- **Incident Response:** How the County responds and escalates responses during critical security incidents.
- **Threat Response:** How the County responds and escalates responses during critical security threats.
- **Resilience Processes:** How the County implements business continuity management and IT disaster recovery planning and testing to protect the resiliency of its infrastructure.
- **Audit Processes:** How regular internal and external audits verify compliance with corporate policies, standards, and procedures.
- **Network Perimeters and Zones:** Determines what network perimeter mechanisms are used by the County to enforce zone boundaries and protect sites, systems, and users across a distributed infrastructure. How zones of trust used by the County to protect their IT resources on communications networks. How the County detects and responds to security incidents on their network.
- **System Zone Placement:** How the County places systems in security zones.

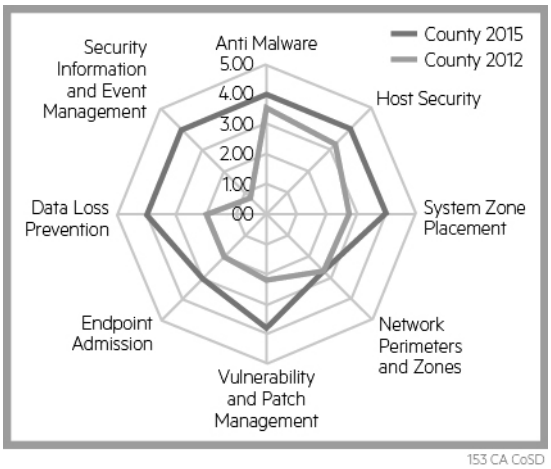
- **Endpoint Admission:** What approaches the County uses to control client endpoint admission to zones and resources.
- **Host Security:** What management and protection postures the County takes with regard to host system security.
- **Vulnerability and Patch Management:** How the County manages and remediates data, software and configuration vulnerabilities.
- **Anti-Malware:** What mechanisms and approaches the County uses to mitigate malicious software such as viruses, spyware, and Trojan horses.
- **Data Loss Prevention:** What approaches the County uses to prevent the unauthorized exfiltration of company confidential information.
- **Security Information and Event Management:** How the County monitors the network and critical systems, including audits of critical system access and logs.

The areas of focus are then evaluated based on key indicators that help determine the Gartner maturity level that represent increased capabilities described below:

- **Level 1:** Initial/Ad hoc — The County's management is aware that security is weak and represents unacceptable risks; information security activities and controls are ad hoc and typically uncoordinated and IT-focused; in many or most cases no formal information security program is in place.
- **Level 2:** Developing/Reactive — An individual has been designated with informal responsibilities comparable with those of a CISO; the County is working to develop program plans and policies; stakeholders are beginning to communicate informally about information security issues; there is some coordination of controls across policies, functions, business units or infrastructure layers.
- **Level 3:** Defined/Proactive — Policies and rules are in place and some information security roles and responsibilities have been established; accountability or enforcement remains minimal, limited, or constrained to specific functional areas; IT efforts and controls are still IT-focused but coordination is widespread (although not comprehensive); security awareness is growing but still limited.
- **Level 4:** Managed — Information security roles and responsibilities are now clearly defined and a formal information security committee—led by the CISO, with participation from the lines of business—has been established; the County is moving away from an IT-centric approach to information security and toward a more strategic defense-in-depth approach; however, line-of-business owners or functional departments have not yet accepted explicit accountability for residual risk.
- **Level 5:** Optimized — Line-of-business managers have now explicitly accepted residual risk and are fully accountable for security failures and policy violations; continuous self-improvement practices are in place across multiple domains; management is provided with incentives to create a security-aware culture in their organizations.

Additionally, Gartner maturity methodology provides the County with peer values with the same organizational profile for comparison. Gartner maintains that this model is based on risk indicators identified by other organizations such as the International Organization for Standandarization (ISO), the SANS Institute, the Institute of Risk Management (IRM), and the U.S. Government Accountability Office (GAO). The indicators to differentiate risk profiles for peer group selection

Figure 11. HPES Gartner's Security Assessment



This assessment provides for continual year-to-year security improvements.

include potential impact to public safety, potential impact to macro-economic and micro-economic stability, cybercrime or hacktivism, if the organization has been previously attacked, and if the organization represents a symbolically significant target.

An example of Gartner's maturity assessment of the County's security program is illustrated above in Figure 11.

- Automated Tools – Automated systems and tools involved in proposed solution

Table 10 is a list of the automated toolset used in the County environment today, and will be continued in the subsequent Contract. Additionally, this will be implemented as technologies and capabilities evolve.

Table 10. Automated Toolsets

TOOL NAME	NOTES – DATA
Governance, Risk Management, and Compliance (GRC)	GRC tool to track policies, processes, master control catalog, systems and how they address security requirements. Additional information includes dashboards, computer security request forms, and other reports.
Risk Radar	Risk Radar is a custom-developed tool to track identified vulnerabilities to make sure they are in the process of mitigation. The tool also tracks the assessed risk for each vulnerability as well as the overall risk for the County.
CCS – Symantec Controlled Compliance Suite	The CCS tool is used to track non-compliant items resulting from HPES policy compliance scans.
Scanning Tools	Scanning tools are used to identify vulnerabilities and determine the level of risk that a specific vulnerability represents.

- Qualifications and Experience – Background and experience in comparable environments

HPES has a rich history in all matters pertaining to IT security and security management. Operating effectively across multiple Federal, state and local enterprises, including NGEN, FDA, FBI, and the City of Anaheim.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

We will continue using/leveraging our current tools, assets, and best practices.

2.5.4.1. What methodology does your organization propose to protect the security and confidentiality of data and information that is proprietary to the County or subject to special statutory protection, including, but not limited to, confidential data relating to health and human services and public safety?

Protecting confidential or sensitive information is a top priority for HPES, we have put in place a robust flexible set of risk-based security methodologies to protect the County's information systems and assets. As previously described, HPES uses the NIST RMF, Defense-in-depth, and the Gartner's IT Maturity Model. Additional guiding principles currently in-place include the minimization of the use, collection, and data protection of what is strictly necessary to accomplish county's business. HPES will support the County-classified data each system is processing or storing and appropriately determine the levels of protection based on the data classification and impact to the County. The appropriate levels of safeguards will then be implemented based on the data classification. Additionally, a robust set of processes and procedures are currently in place to handle incidents involving the compromise of the data. HPES

encourages close coordination between County officials, such as the CIO, Chief Privacy Officer, CISO, with HPES counterparts to make sure that complex laws and regulations translate to effective policies, technical security controls, and the implementation to protect the data across the enterprise.

The NIST-based RMF fundamental tenets of security include controls that are specifically designed to protect the confidentiality and integrity of data. At a high level, the controls include the creation of policies and procedures, awareness and training, conducting Privacy Impact Assessments (PIA), identifying and classifying sensitive information, and record retention and disposal of information. Other control specifics include:

- **Access Enforcement** – The County controls access to confidential data through access control policies and access enforcement mechanisms. At the enterprise level, employees are part of role-based Active Directory (AD) groups which are determined using a Change Security Request Form with approval and consent of a direct employee supervisor. Other non-enterprise systems control access with local management capabilities. As part of the roadmap, a full enterprise identity management capability will be in place to better secure and manage access controls.
- **Least Privilege** – HPES will enforce the most restrictive set of rights and privileges for each user in a specific role. For confidential information, HPES makes sure that users only have access to the minimum about of data needed to perform their job.
- **Auditable Events** – HPES will monitor events of systems that contain confidential information and will make sure there are regular reviews and analysis of system records that indicate inappropriate or unusual activity affecting this data. Investigations will occur when suspicious activity is detected and violations are reported.
- **Identification and Authentication** – County users will be uniquely identified and authenticated before accessing confidential information.
- **Media Access** – HPES will restrict access to media containing confidential information, often through encryption. Media includes CDs, USB flash drives, backup tapes as well as non-digital media such as paper.
- **Media Transport** – HPES will protect digital and non-digital media including confidential data transported outside the organization. A data transfer request process will be used to scrutinize the data (often encrypted) that leaves County premises.

All of these sets of controls will be implemented at the infrastructure level and on applications that process confidential information. The visibility of how effective controls are being on the lookout for new threats, identifying vulnerabilities, and having a sound mitigation strategy to eliminate or minimize risk will result in an optimally protected enterprise.

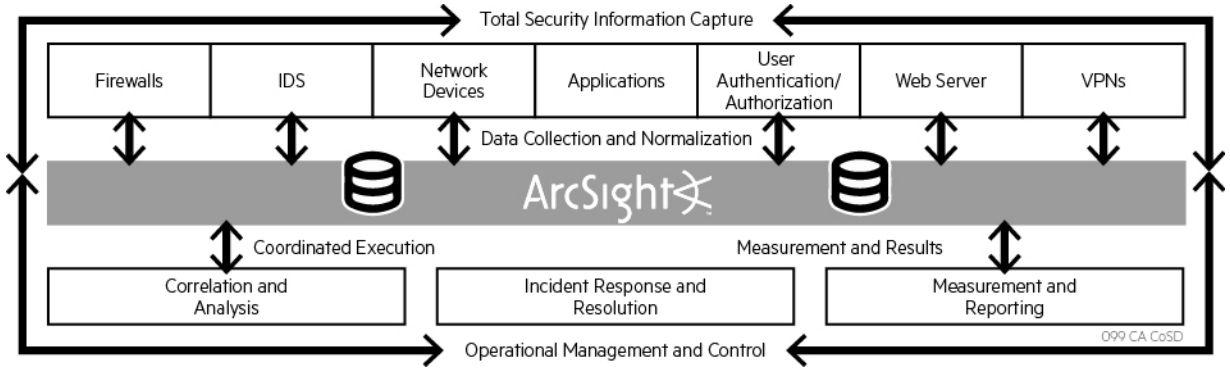
2.5.4.2. Describe your proposed approach to data analysis of SIEM information and remediation of identified risks or vulnerabilities.

The major components that will comprise the HPES SIEM solution are: monitored endpoints that generate security events, security data collection servers that collect and normalize events from disparate endpoints, a security information event manager backend that correlates and analyzes collected events and a web portal that presents processed events and alerts. Finally, the SIEM solution will include security incident response processes to coordinate analysis and resolution of security issues.

HPES will use the ArcSight platform, illustrated in Figure 12, to perform the aggregation and correlation of security events generated by different data collection points. Palo Alto logging (traffic, threat, and URL) is collected by the Palo Alto centralized managed server platform, Panorama. All SSLVPN logging, as well as DHCP logs will be gathered by the Juniper JSA device. These two devices then forward their logs to both the HPES SIEM (ArcSight) collector, as well as the AT&T managed SOC group. Data center logging (IPS sensors and firewalls) is also fed to the HPES SIEM. HPES will analyze

and resolve issues to provide an additional layer of security. An event alert from either group triggers a collective investigation effort between HPES and AT&T.

Figure 12. ArcSight Platform



The ArcSight Platform provides tool information security capture, coordination, management, and reporting

At a high level, the process to escalate and respond incidents is as follows:

- The HPES security team will investigate alerts, determine criticality and, if the criticality is severity one or severity two, will notify the County and HPES security about the event. If the event does not meet critical criteria, the HPES internal procedure for noncritical incidents will be followed and reported to the County in the monthly security reports.
- In the event of a severity one or two, HPES will initiate the investigation and contact the County CISO and HPES operations or any support team requested to alert them of the incident per the Severity Escalation Matrix.
- HPES will investigate the incident and activate an incident response team (IRT) as needed. If the documented preapproved, incident containment strategy exists to mitigate threat, the IRT will immediately execute plans to resolve incident.
- The IRT determines resolution strategies for County approval. If required, the team will initiate the change management process by submitting requests for change (RFC).
- The IRT will execute a containment strategy upon approval of an RFC, if required. The strategy will include plans for the prevention of further damage caused by the incident and will be reviewed by the County CISO.
- The IRT will execute eradication strategies when the RFC is approved and reported to the County CISO.
- The IRT will execute recovery strategies upon approval of RFC by the County CISO.
- HPES will document the incident and close the incident.
- HPES will conduct a lessons learned meeting to update strategies, as needed.

Each process of the SIEM incident response will be included in the yearly review process, which will contribute to the maturity of security services. Any areas of improvement or lessons learned will be incorporated in the updated process and teams will be aligned accordingly.

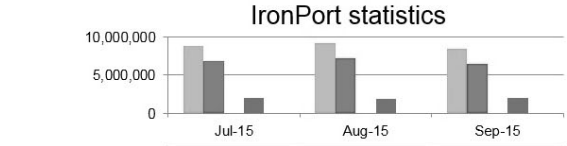
2.5.4.3. Describe your proposed approach to assess the County's security environment.

HPES employs multiple approaches to continually assess and protect the County's environment. HPES will continuously monitor in real-time mail threats, inbound and outbound network traffic, and discrete data formats in which information leaves County's networks. Additionally, HPES' ESOC will respond to any possible threat by investigating whether it is a true incident or if it is a false positive. False positives

are used to constantly fine tune IPS/IDS and the heuristic engine for data analysis. Figure 13 illustrates typical quarterly County statistics of such events.

Figure 13. Typical Quarterly Security Events Monitor

Threat	Technology	July	Aug	Sep	Q3 Totals	Status
Blocked Mail Threats	Ironport	78%	79%	76%	77.67% of total traffic blocked	Healthy
Email Investigations - Spam/Phishing/Web Content	Ironport/Exchange	92	85	87	264 Investigations completed	Healthy
- False positives		85	82	84	251 False positives	Healthy
- Incidents		7	3	3	13 Blocks added	Healthy
Firewall IPS Threats – Tulsa/Plano	Tipping Point IPS	5	3	10	18 Investigations	Healthy
- Normal Traffic		4	3	10	17 Normal Traffic	Healthy
- Failed Attacks		1	0	0	1 Attack stopped	Healthy
Firewall IPS Threats – San Diego	Juniper IPS	0	0	0	0 Investigations	Healthy
AV Threats	Symantec Endpoint Protection	0	2	2	4 Investigations	Healthy
- Quarantined/Deleted		0	2	2	4 Eliminated	Healthy



	Jul-15	Aug-15	Sep-15
Q3 Total Inbound	8,873,444	9,178,566	8,472,577
Total Threat Messages	6,888,925	7,284,885	6,426,462
Threat Percentage	78.00%	79.00%	76.00%
Total Clean Messages	1,984,313	1,893,461	2,045,867
Clean Percentage	22.00%	21.00%	24.00%

Hewlett Packard Enterprise

Improving security through method-based tools and automated processes

Vulnerability scans will be conducted for a maximum of 3,000 IP addresses in the DMZ zone as well as the library network. The plan is to increase the number of servers to include all critical servers based on function and data classification they store or process.

Additionally, HPES conducts scans of servers before they go into production, which results in identification of vulnerabilities in servers before they go live. High and moderate vulnerabilities will be mitigated before any server goes into the production environment.

HPES conducts policy compliance scans on all production servers on a monthly basis. These scans will make sure County servers are compliant with HPES security policies and are up-to-date with patches.

Another way of assessing the security posture of the County is by executing an annual network penetration test restricted to the DMZ. The HPES network penetration testing process includes actions that reduce the risk of exposure to the County's most critical online assets and, detailed descriptions for quickly managing or eliminating security exposures. This streamlined, granular approach to risk management enables security policy compliance to become an integral part of the overall security process.

Complementing all the efforts described above and as part of the RMF, environment controls will be documented and tested on a predefined efficient schedule. HPES will assess the security controls using appropriate procedures to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the County. The ongoing monitoring of security controls in the environment will also include documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate County officials such as the CISO, CIO, and CTA.

Finally, and most useful at the executive level, HPES and the County CISO will continue to conduct monthly self-assessment using Gartner's IT Maturity Model and report to the County via CIO briefings. This will provide independent validation to the County of HPES' performance.

2.5.4.4. Describe your proposed approach to assess the County's application vulnerabilities and security risks, and your proposed approach for analyzing and assigning classifications to County Data.

Checklist Based Approach

The application checklist is a documented set of questions based on County security policies with the goal of identifying areas in which the application under review is not compliant with specific security requirements. The requirements on which the application checklist will based are documented in the County Security Management Plan.

The compliance questions will be are categorized into the following security areas:

- Authentication
- Audit
- Nonrepudiation
- Host security
- Enclave
- Access Control
- Confidentiality
- Physical Security
- Application Security
- NIST
- Support
- Integrity
- Network Security
- Data security

Application team members will respond to an extensive set of questions at different stages of the project and the list will then be reviewed by the security team. A scorecard is then derived from the questionnaire that is rolled up to a dashboard for all applications going through this process. The dashboard facilities identifying trends within specific security categories across multiple applications.

RMF-Based Approach

Applications will go through the RMF, as described at the beginning of this section. All applicable controls will be determined by the data classification and take into account factors such as compliance with HIPAA, Privacy, PCI, and other applicable laws and regulations.

Comprehensive Applications Threat Analysis (CATA) – Optional Transformation Project

Selected high-risk applications will use a Comprehensive Applications Threat Analysis (CATA) service, which is intended to reduce the risk of the introduction of undiscovered (latent) vulnerabilities and security defects during the application development life cycle, in the application itself, and determine whether the data is adequately protected by the application. CATA can also be applied after development to identify future security updates that could or should be applied to the application or to provide a high-level Independent Validation and Verification (IV&V) assessment of the risk of security vulnerabilities at the requirements, architecture, and design levels. As more vulnerabilities and their exploits are discovered, protecting critical data becomes a never ending battle. CATA reviews will be necessary to determine if the current application architecture and code base remain secure.

CATA begins with a security requirements gap analysis—an analysis of an application to map often-missed regulatory security requirements into technical security requirements imposed on customers by relevant laws, regulations, or practices.

The next step is an architectural threat analysis—an analysis of an application architecture and high-level design to identify changes to reduce risk of latent security defects to a uniform acceptable level by identifying areas of high/medium architectural risk and then lowering that risk. The output of this step is a prioritized and vetted list of threats and an action plan to remediate.

Together these steps are called the HPES CATA. We will use the results of this analysis to identify areas in the architecture of greatest risk to provide a risk-based prioritization, which can also provide input into security testing and security code review methodologies.

Encryption Requirements for Data Security and Protection

HPES over the years has continually moved toward encrypting County data using several encryption methods, technologies, and in different layers. Following is a breakdown of encryption used in our proposed solution to protect data in transit, at rest, and the PKI Enterprise implementation.

- Data in transit
  - Transport Layer Security (TLS) – Web servers use TLS with digital certificates provided by Entrust.
  - Secure Sockets Layer (SSL) – Web servers use SSL with digital certifications provided by Entrust.
  - Server Message Block (SMB) – Applied to Windows shares (NAS) and files in transit.
  - Virtual Private Networks (VPN) – Junos VPN uses IPsec tunnel. Traffic between the two points is encrypted.
  - Wireless Encryption – Wireless Access Protocol provides encryption on all wireless data exchanges.
  - Email Encryption – TLS to all inbound connections and to trusted outbound domains. Cisco IronPort Outlook plugin.
  - Mobile Devices – SSL encryption for all communications with County network when using Pulse VPN. Email is encrypted using TLS inbound and outbound when accepted by both parties.

- Data at rest
  - Endpoint Encryption – Symantec Endpoint Encryption provides maximum protection by encrypting each hard drive sector by sector.
  - Database Encryption – Transparent Data Encryption is used in some SQL databases.
  - Removable Media Encryption – Thumb drives ordered from the catalog use AES 256-bit encryption.
  - Password Hashing – New applications or modified during refreshes that store passwords use hashing algorithms to prevent storage in clear text.
  - Mobile Devices – Devices are encrypted using the Operating System default encryption capabilities where appropriate. Additionally, devices will use a digital certificate to authenticate to AirWatch.

- PKI
  - User Authentication – Symantec Digital Certificates in Active Directory. (In progress)
  - Device Authentication – Symantec Digital Certificates in all devices. (In progress)
  - Digital Signature – Self Signed Digital Certificates by ARX and CoSign. (In progress)
  - Other use cases will leverage the current Enterprise PKI Symantec solution.

HPES is aware that some of the legacy applications and technology do not use encryption in all cases. It is our intention to continue to implement solutions with encryption where technology allows for it. Opportunities to improve in this area include technical refreshes and new implementations.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

No alternative approaches were identified

2.5.5 Service Delivery Management (Sched 4.3, Section 2.7)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

As the current provider, we have worked in collaboration with the County for years to make certain that the services provided under Service Delivery Management are the right fit to meet the County's business needs. The foundation of HPES' Service Delivery Management model is based on ITIL certified processes, combined with our experience/expertise in performing these services for the County. The approach features repeatable, ITIL compliant, delivery of County IT services that consistently provide high-quality IT service delivery across all frameworks. The County will continue to benefit from HPES' globally established and proven approach as we continue delivering optimized and standardized IT services.

Our Service Delivery Management services will be applied and enforced by our enterprise service delivery manager along with the individual service delivery managers (SDMs) assigned per business group. We will continue our delivery of these services through proactive communication and collaboration with all affected stakeholders. In addition, we will provide timely guidance and measure results accordingly as required. We will document our efforts and make this documentation available on our service delivery portal. We will routinely solicit County and end-user feedback as input into our continuous improvement processes, as we do today and as we move forward. Key to this approach is to be transparent and collaborative, and to thoroughly document at all levels and milestones. Our deep familiarity with County IT services requirements and future needs confirms our approach and proposal of the following Services Delivery Management solution and accompanying rationale.

Solution: While ITIL certified processes and collaboration will be the foundation for our processes and approach, the key element is assigning a single service delivery manager (SDM) to be the point person for each business group. This service had been provided to the County previously and was proven to be very valuable to the account and to the customer, giving each business group a single point of contact to reach out for assistance with any of their business needs and requirements. SDMs will perform most of the duties the incident managers do today in the current model and will include the following at a minimum:

- Incident management
- Problem management
- Change management
- Release management
- Escalation management/Service Request status
- Communication
- Billing management
- Availability and capacity management
- On-call rotation

The on-call rotation in which the SDMs participate is critical to facilitate centralized after-hours support to the County for issue resolution as well as making sure each SDM has appropriate amounts of time off and vacation as required. HPES is proposing five SDMs who will rotate on-call every five weeks. During

business hours (Monday through Friday 6:00 a.m. to 6:00 p.m.), each SDM is responsible for their own business group. After hours and on weekends, the on-call SDM takes primary responsibility for any issue and works it to resolution. If an enterprise issue emerges during business hours, the on-call SDM takes point for this issue initially—and possibly to completion, depending on the scope of the issue. If an issue arises during this time within the business group for that on-call SDM that requires their focus and attention, another SDM will be assigned to take over the new issue. All SDMs from each business group will be required to work any/all enterprise related issues/disasters that require a shift rotation. The on-call SDM will verify that the correct customer from the business group is notified and that the SDM assigned to that business group is aware if anything has occurred in their space so they can address it. Problem management is a day-to-day responsibility for the SDMs, and they will be assigned activities to work whether it be proactively or through tickets, escalations, and so forth. HPES has a primary owner—the enterprise problem manager—who will report, track, and communicate all problem management issues worked by the team and the account as required in the weekly CTO Operations meeting. Each SDM will also report any problems being worked by them through this process that impact their business group or the enterprise in the monthly portfolio review meetings that they will be required to attend.

For capacity management, each SDM will be responsible for using report-based findings and data to facilitate the health of their servers and applications for that particular framework. Our SDMs operate proactively make certain this health is sustained, reliable, and predictable. They work closely with the capacity manager on the account who owns the activities and verifies that we are resolving alerts as well as reviewing trends to implement the right steps to prevent alerts and to make recommendations to County stakeholders.

HPES has a single point of contact on the account responsible for Root Cause Analysis (RCA), making sure that all RCAs meet the required deadlines and service level agreements (SLAs). As issues are worked—for those that require an RCA or for which an RCA has been requested—the SDM for each business group makes sure that they are completed within the SLA timeframe and they are ready for customer review and approval.

Each business group has regularly scheduled meetings that the SDM will be required to attend and report status as needed for all things operational and that fall within the scope of their duties. Because the SDM acts as a point of escalation, they will assist the client with answers and resolutions by establishing the proper points of contact and making sure the issue is being worked or obtaining and providing the information required.

If an emergency or disaster occurs in a specific business group, the SDM for that unit takes primary responsibility as needed to support the customer. They handle the requests, communications, and so forth required for these events. If the event is something that requires 24x7 support, we will provide the necessary resources to cover shifts and see that the SDM has adequate support. If an emergency is declared that impacts the entire County and the Office of Emergency Service (OES) activates, the SDM for the Public Safety Group (PSG) space begins the rotation along with the enterprise service delivery manager to establish required communication and coordination, and the SDMs enter that rotation along with account management to support the effort until we are notified to stand down.

Our Enterprise Service Delivery Manager (ESDM), Kathleen Barghols, is responsible for leadership of all SDMs; she understands their duties and provides continuity across the business groups and the account. The ESDM has a direct interface with the County Technology Office (CTO) to make sure that all parties are aware of anything that is going on in the environment and to make process changes/suggestions as needed for continuity of operations. The ESDM is embedded with the customer three days per week in the CTO and will attend all business group meetings as requested. The ESDM is responsible for all delivery aspects and SLAs associated with each area for the account on the operational side: service delivery management, service desk, end user, infrastructure services (data center and local), print center, network

services, release management, change management, problem management, incident management, and configuration management.

Rationale: HPES has in place a well-documented and robust service delivery management process. Our *hands on* experience with the County confirms our proven service delivery management services solution and validates its continued usage. Essential to our successful approach are the trusted and transparent relationships our SDMs maintain and nurture. These individuals come from a pool of existing resources on the account that already have established relationships with the end users as well as a deep level experience in the County's business. This is the same staff that we have in place today for incident management in our Infrastructure Operations space that helped the account achieve the highest scores we have ever seen in the Voice of the Client Survey that was conducted in 2015 for these services.

The SDMs are responsible for understanding all service frameworks and how they impact their business group as well as for making certain that proper communication and discussions for that framework take place and that resources are available to support all service delivery initiatives. The SDMs are familiar with and facilitate adherence to County requirements and information infrastructure; they will seamlessly continue these best practices on the new IT services contract.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

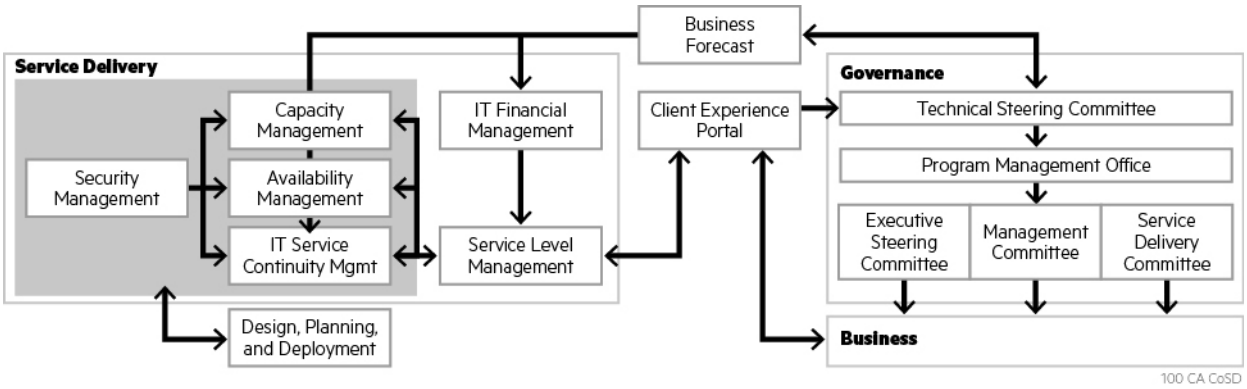
The SDMs are required to have face-to-face interaction with their business groups in addition to email, phone, etc.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES' approach to service delivery, illustrated in Figure 14, enhances the stability and integrity of the services environment through proactive service-level management and governance, transparent service visualization, and analytics that support cost-effective service improvements through integrated availability, capacity, IT service continuity, and financial management. They include the following key service delivery disciplines:

- **Availability Management** – The mission of availability management is to understand the availability requirements of the County and to plan, measure, monitor, and continually strive to improve availability of the services and the County's IT infrastructure.
- **Capacity** – HPES performs capacity planning regularly as well as when new business and application growth are anticipated, when changes to the existing business are anticipated or occur, or when configuration changes are performed within the systems. As part of our ongoing capacity review and planning process, HPES will coordinate with the County regarding future business plans and computer resource requirements.
- **IT Service Continuity Management** – HPES' business continuity professionals will collaborate with the County to keep its IT Service Continuity Management (ITSCM) plans current, relevant, and executable and to see that they support County operational continuity plans.
- **Service Level Management (SLM)** – The County and HPES establish a shared view of the services, service-level achievement, and analytics through regular service delivery reviews and IT Service Management (ITSM) Client Portal dashboards. HPES' account leadership team will collaborate with County stakeholders through service delivery reviews and frequent direct dialog to continually review SLAs to make sure that services remain cost-justified and aligned to the County's business needs. The ITSM Client Portal provides continual "Voice of the Client" feedback to HPES and relays performance feedback at any time, with top-level visibility to HPES' senior leaders.

Figure 14. HPES' Service Delivery Model



Service delivery integrates availability, capacity, IT service continuity, IT financial, and SLM to enhance the stability and integrity of the services environment.

The following sections provide additional detail about the service delivery processes depicted in the diagram and summarized above in Figure 14.

Availability Management

The ongoing process of availability management is to plan, measure, monitor, and continually strive to improve the availability and the stability of existing services and County infrastructure to prevent the occurrence of outages and delays. Availability management contains the following key activities:

- Assess availability requirements
- Develop and maintain the Availability Plan
- Analyze current availability
- Maintain availability

Capacity Management

Our goal is to provide the County with a sustainable, reliable, and predictable environment. HPES performs capacity planning regularly when new business and application growth are anticipated and when changes to the existing business are anticipated or occur, and when configuration changes are implemented in the systems. We are successful when we are able to meet the County's capacity demands with complete transparency, and prevent outages. Capacity management is discussed in detail in Section 2.5.12. Capacity management supports the following key objectives:

- Verify that optimum IT capacity exists always
- Proactivity
- Reliability
- Outage prevention
- Provide clients with sufficient capacity to support agreed levels of service
- Forecast future requirements for IT resources.

Service Continuity Management

HPES business continuity professionals will work with the client to be sure that ITSCM plans are current, relevant, and executable and that they support the County's business continuity plans. The ITSCM process comprises the following key elements:

- **Define, Implement, and Maintain the ITSCM Plan –** HPES collaborates with client business continuity teams to define, implement, and maintain an ITSCM plan that is based on Disaster Recovery Institute International (DRII) and Business Continuity Institute (BCI) standards. The plan is continually updated and assessed through scheduled reviews, as changes are made to the IT environment and as improvement opportunities are identified through testing and execution of the plan.
- **Exercise and Execute the ITSCM Plan –** HPES' IT service continuity staff will support the client when conducting required testing and activating plans during a disaster. HPES will document and maintain the HPES staff's IT service continuity procedures to restore the hardware and operating system and the subsystem environment. HPES operations will support application recovery testing, such as loading tapes or initializing data storage devices. Joint testing of the IT service continuity plans is conducted through a disaster simulation process based on established test schedules. We closely monitor and document test objectives and actual test activities. We review the results of each test and enter any problems encountered in the problem-tracking tool for follow-up and implementation of corrective action. This process enables continual improvement of the recovery plans. Retests will be performed for tests that do not meet predetermined objectives unless mutual agreement deems retest to be unnecessary.
- **Manage Service Continuity Escalation –** Throughout a service continuity event, HPES will manage the agreed escalation procedures to keep the client and HPES leaders informed, obtain required approvals, and restore service operations in accordance with service levels, thereby minimizing the impact to business operations.
- **Supplemental Assets –** Available for use on the County's program, HPES has ITSCM-based templates for documenting the following: Business Impact Analysis, Gap Analysis, Continuity Planning Checklist, Threat Analysis, ITSCM Plan, and ITSCM Exercise Workbook.

Service Level Management

HPES' delivery team will focus on providing service excellence at agreed levels. We will track the associated metrics and analyze results to determine not only how to best meet our commitments, but also to proactively discover new approaches that lead to greater service efficiency. We will work with the client to verify that the levels of service we deliver meet County business objectives.

Security Management

Drawing on our past experience with the Defense Information Systems Agency (DISA) including support of the associated DoD Information Assurance (IA) controls and our experience in the DoD environments, HPES will complete a Security Management Plan (SMP) modified from our proven template to identify those security-critical items whose failure could lead to a breach of system security. We will document a security assurance strategy to minimize or eliminate the potential for system security breaches. We will review and update the SMP as necessary throughout the program life cycle.

HPES is currently performing security management satisfactorily for the County. We will continue this service on the follow-on contract, as we provide a seamless transition with no degradation in services.

- Automated Tools – Automated systems and tools involved in proposed solution

The automated tools HPES will use in providing support to the County are as follows:

- HPE Service Manager
- Project Management

- Qualifications and Experience – Background and experience in comparable environments

HPES is 100% of the incumbent team supporting the Enterprise Hosting and IT Infrastructure Service areas. Our strong personnel qualifications include the current data center operations manager, team leads,

and technical subject matter experts with in-depth knowledge of information technology/information management (IT/IM) Government personnel, customers, and processes as well as proficiency with IT/IM hardware, software, networks, applications, databases, processes, and tools.

In addition, HPES has reach-back capability to in-house resources to support growth in staffing requirements and to support transition periods. HPES is focused on—and committed to—aligning cost-effective services for enterprise hosting and IT infrastructure that achieve County customer satisfaction within budget and on schedule with minimal risk. HPES possesses a wide breadth of management and technical capabilities and will provide the "one-stop shop" with a single point of accountability.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.5.1. Describe your proposed approach to the role of the Service Delivery Manager (SDM), including SDM operational authorities across Service Frameworks, key functional activities, and metrics to measure the effectiveness of the SDM role.

The SDM role is responsible for managing the successful execution of the County services delivery that can be achieved only through time-tested, trusted and transparent working relationships. The SDM will work closely with counterparts from the County team, outside vendors, and HPES teams to facilitate a successful initial and ongoing services delivery engagement. This role—essential to managing a small team of technical and business people—requires varied expertise in the areas of technology, business processes, communications, service provider, and enterprise IT industry knowledge and experience. Essential to this role is serving as the face of HPES services on an ongoing basis for the County in all aspects from supporting pre-design activities and design to delivery, process improvement, and escalation management. Customer relationship management is a central and key requirement for all HPES SDMs. We instill in them the premise that "we have to earn the right to do business and to demonstrate that we care."

SDM responsibilities and deliverables include the following:

- Serves as primary interface for all client contact related to the HPES services, involved in pre-design and post implementation interface with County and HPES services leadership teams
- Responsible for County relationship management and total customer experience
- Works closely with senior management and across functional groups to develop effective strategies and programs to meet service delivery goals, including tracking and reporting key milestones
- Responsible for making certain that HPES complies with agreed services scope and quality
- Provides compliance with established policies, practices, and processes defined by HPES and County personnel for delivering converged infrastructure related services
- Provides work direction and strategic direction to reporting managers and employees
- Works closely with HPES lead partners in ensuring a successful services delivery engagement

Metrics to measure SDM effectiveness include the following:

- County leadership evaluations—the GITM and ESDM will meet quarterly at a minimum to discuss how the SDM is providing the services required
- Project performance to goals and objectives
- Meeting scheduled reporting and communication deadlines
- Maintaining agreed certifications
- Annual Performance Reviews by the ESDM
- Customer relationship management skills and meeting objectives
- Identifying opportunities for improvement within their respective business group

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

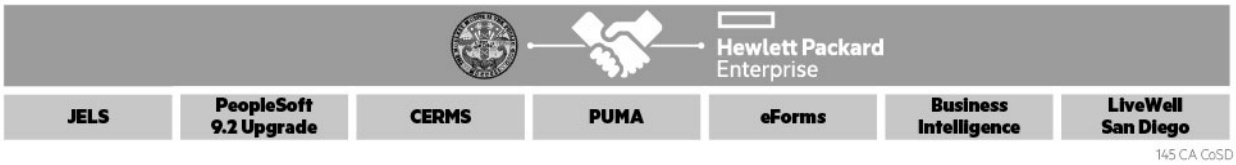
2.5.6 (Reserved)

2.5.7 Project Management (Sched 4.3, Section 2.9)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The HPES Enterprise Project Management Office (EPMO) is an organizational body assigned to centrally coordinate the management of in-flight programs and projects across all towers of the County ITO contract. Through more than 10 years of successful Project Management for the County, our combined teams have developed a quality base to build on for our next generation agreement. Since 2011 our team has completed more than 5,000 project initiatives for the County. Significant and award-winning projects have helped drive County success stories and HPES is proud to stand with the County on these accomplishments.

Figure 15. Enterprise Project Management



Solution: The EPMO is responsible for aligning its activities with the County's mission and maintaining an outcome-focused and metric-centric program management organization. To accomplish this, our approach incorporates measured steps to retain situational awareness of the budget, schedule, and risks as well as opportunities for continual improvement throughout the program's life cycle. Our EPMO strengthens day-to-day communications and prepares detailed recurring reporting to promote the highest level of transparency and collaboration between the County and HPES.

HPES uses industry-standard practices as set forth by the Project Management Institute (PMI's PMBOK), Software Engineering Institute (SEI's CMMI), and Information Technology Infrastructure Library (ITIL). HPES has its own Enabling Delivery and Global Excellence (EDGE) process, which is our overall framework for enhancing effective planning, execution, tracking, and reporting of projects. The HPES Team uses one or more of these best practice standards to create procedures that enable each framework to efficiently perform project management activities appropriate for the nature of our work.

HPES EPMO guiding policies include:

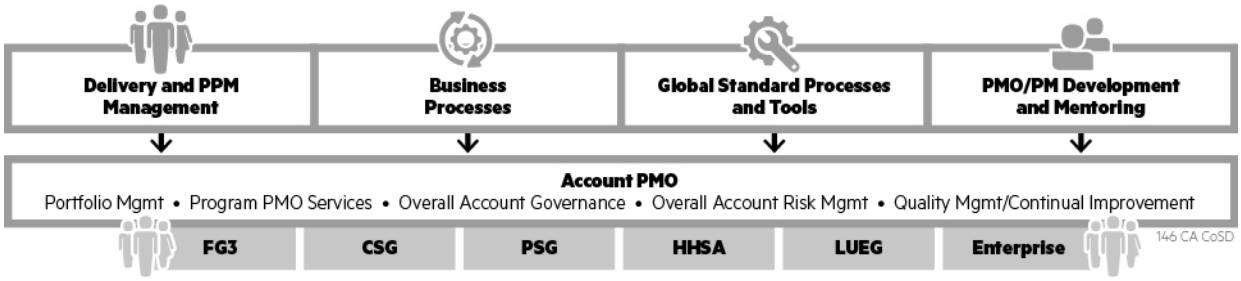
- Identify and use global best practices as a framework for creating tailored, relatable, and customer-centric procedures that provide the best fit to meet our customers' evolving needs, while driving quality and expedience into our delivery model.
- Provide frequent, accurate updates to the County Project Sponsor
- Make sure of thorough and timely communication across all framework projects and procedures
- Apply the principle of delivering projects on time and within budget that fulfill the approved requirements
- Promote an environment of continuing education for Project Management Professional (PMP)-certified PMs and for those who aspire to be PMP certified
- Work with our County partner on continuous improvement processes and initiatives.

These policies are designed to influence and determine decisions and actions when tailoring the processes for the County and ensuring that our processes conform to PMBOK, CMMI, and ITIL.

The EPMO chairs weekly meetings to make certain that cross-framework coordination, integration, and communication occur for projects and processes. Communication between all frameworks is critical to successful delivery of products and services. Figure 16 shows communication between the EPMO and the frameworks.

The EPMO is committed to coordinating multi-framework projects between the frameworks, and to certifying that there is a lead project manager and project status is reported in a timely and consistent manner. EPMO will provide a central point for managing processes and standards across all frameworks to enable consistent delivery.

Figure 16. EPMO and Frameworks Communication



Effective communication between the EPMO and all frameworks is essential for contract success.

HPES proposes the development of a formal process change board to identify and implement process improvements that drive quality and expedience throughout the project life cycle. The HPE EPMO would chair these efforts and support documentation, training, and process reengineering that may be identified through these efforts.

In addition to the standard project management solution described above, HPES has also taken this opportunity to offer additional value to the County customer by consolidating Infrastructure Project Management efforts, which were previously part of the monthly server RUs, into our project management service. This will provide value to our customer while continuing to facilitate HPES' goal to integrate all project management services under one set of best practices.

Rationale: Knowing the County's wants and needs through experience, we can be flexible in our approach while still holding all parties accountable to regulations and best practices. We will maintain a cooperative relationship with the County. HPES institutionalizes our processes, but we are also focused on creating an effective customer-centric solution. We know that the processes must support the business and not institutionalize cumbersome bureaucratic practices that hinder efficient delivery.

The EPMO will drive the standards for project management across all portfolios, but will remain agile where necessary to meet the needs of the specific project/client. Our approach of using proven PMBOK and ITIL processes in combination with our knowledge of the County and its business has led to a successful partnership between HPES and the County for the past 5 years. We look forward to continued improvements (specifically with respect to "speed to deliver") and growth based on this strategy.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The EPMO and project management staff will be centrally located at the HPES Rancho Bernardo facility. We will join the County at its facilities when necessary to drive successful communication at the program

and project levels. This facility approach enables interaction between the project management staff and all customer and HPES portfolio towers, including:

- County Technology Office (CTO)
- County Group IT Management (GITM)
- County Department IT Coordinators
- County Project Sponsors
- HPES Account and Operation Management
- HPES Applications Portfolio Management
- HPES Infrastructure Operations
- HPES Account Security
- HPES Technology Office
- HPES Business Management
- HPES Contracts Management

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES' proven methodology for effective program management support, EDGE, includes all information needed for Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE supports all individuals in each ES business unit by providing best practices that they can leverage and use in their daily work.

The EDGE environment covers multiple life cycles that can be selected, customized, and integrated as needed for each program. Project and program management are integrated through their own life cycles, which conform to PMI PMBOK industry standards, as well as CMMI and ISO. Engineering practices, such as Infrastructure, COTS, and other Enterprise application areas, integrate seamlessly with the Project/Program Management areas for project success. EDGE has been customized to the County's needs and processes. EDGE is regularly updated to provide end users with the most current industry best practices, as well as continually aligning processes and assets with changes in industry standards of PMI, CMMI, ITIL and ISO.

To get the most out of our enterprise methodologies and procedures, we emphasize communication. Our EPMO will communicate directly and frequently with the County CTO and project sponsors to identify the best project management solution at the best value.

Using the aligned HP/County organizational structure, we will implement formal communication procedures that engage internal and County stakeholders. Examples of interactions include the following:

- Establishing communication strategies for the specific needs of the CTO and County business groups
- Developing enterprise communication procedures and templates
- Auditing program and project communication plans
- Creating EPMO announcements followed up by direct communication with impacted stakeholders
- Developing and maintaining communication vehicles such as the EPMO SharePoint
- Creating and executing communication plans for EPMO initiatives
- Preparing presentation material for internal and external reporting.

In addition to communication at the program level, the HPES PMs, as governed by the HPES EPMO, will interact with the County in a number of ways:

- Meet regularly with the project sponsors, County Group IT Managers (GITMs), and members of the County Technology Office (CTO) to review status and discuss project concerns, activities, risks, issues, or needed escalations

- Support County sponsors with remediation efforts as necessary to verify County satisfaction with project performance
- Confirm we remediate and follow through on risk items to the County's satisfaction and successful project delivery
- Partner with sponsors and vendors to deliver a consistent and predictable customer experience.
- Maintain a list of project stakeholders, their role and contact information of all who are involved with the project. This list is distributed to all stakeholders.

- Automated Tools – Automated systems and tools involved in proposed solution

Project and Portfolio Management Center (PPMC) is our Primary Project and Portfolio Management (PPM) tool suite. We use PPMC for the development and ongoing management of project schedules, small project work, LOE-based work, operational support work, budget tracking, and status reporting. We also use it to track program-level, high-visibility initiatives with multiple projects (such as IPTS and PeopleSoft), and at the portfolio level to manage and track projects with competing resource needs within a business group. Many reports from PPM are used by HPES and the County to access the status and health of all projects managed on the account. The primary purpose of the County PPM process is to facilitate County decision-makers in optimizing scarce resources by allocating them to projects that are of highest priority and importance for customers and the County leadership. The PPM process provides a clear construct wherein business leaders can build and manage a sound portfolio that is measured with respect to both business and technical factors such as cost, risk, schedule, and capacity.

- We will use SharePoint as a storage repository for project artifacts, enabling easy access of project standards, methodologies, processes, and procedures; storage and access of project templates; and storage and access of project-specific documentation such as specifications, project plans, etc.
- Basis of Estimate: HPES has developed a unique Rough Order of Magnitude (ROM) tool that the EPMO uses to support expedited and thorough estimates that the County needs to secure funding for its initiatives. This tool is based on PMBOK-defined procedures for estimating while accounting for County-specific processes when developing an estimate. It enables the project manager to define the project work in terms of complexity/risk and a standard list of deliverables and tasks which follow the development methodology selected and client requirements at the early stages of a project. It provides ranges of estimates based on the input and historical estimates and actual effort from past projects. This customized tool takes into account client and HPES processes and life cycles, and documents decisions and assumptions made for planning. This tool is managed internally, and automates the creation of client-facing deliverables, including the Budgetary Estimate Cover (an authorizing document). The EPMO team tracks performance of estimates to actuals on projects and uses that data to further inform and improve the BOE tool and improve the quality of our estimates to the County client.

Table 11 shows additional HPES automated tools and methodologies.

Table 11. HPES Automated Tools and Methodologies

MANAGEMENT TOOLS AND METHODOLOGIES	FUNCTION	
County Enterprise Portal	Acts as the single, virtual, and centralized source of information for all County stakeholders and HP. The Portal will provide access to the following:	
	• Consolidated program reporting • Service levels reporting	Contractual information Contractual deliverables and plans

MANAGEMENT TOOLS AND METHODOLOGIES	FUNCTION
Project and Portfolio Management Center (PPMC)	• Consolidated project management tool • Budget management and labor billing source • Schedule management • Resource management • Risks and issues management • Project status reporting
County Document Repository (DocVault)	Workspace and final repository for all project-related deliverables and account-wide policies and procedures
Program and Project Management Methodology	Includes templates that outline scope, risk, quality process, personnel, cost, schedule, communication, and procurement management responsibilities
Service Delivery Dashboard and Voice of the Client (VoC)	Provides clients with program performance and enables them to provide direct feedback to HPES executive leadership

For internal tools such as the above that are used to the support the County's business, we will conduct reviews of the systems on a semi-annual/annual basis, depending on the tool, to determine whether major upgrades or replacements of systems are required to make certain that we are using the right technology to support the County's needs and remain in supported status.

- Qualifications and Experience – Background and experience in comparable environments

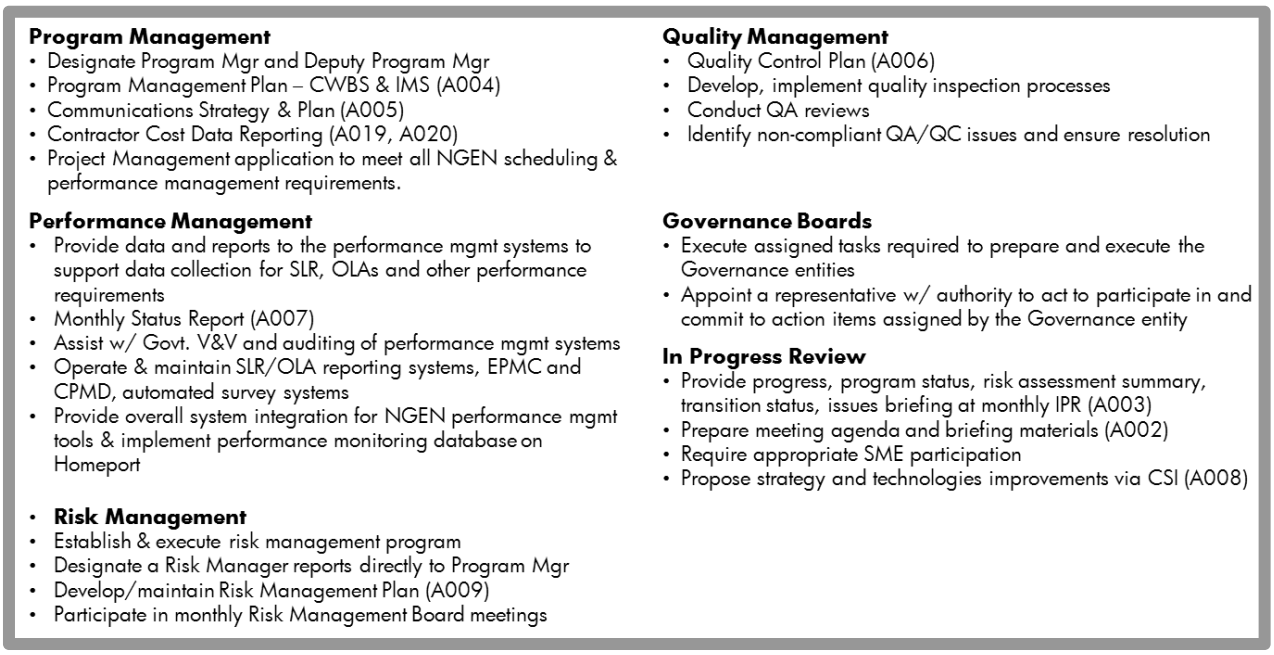
With more than 10 years of successful project management for the County, our combined teams have developed a quality base to build upon for our next generation agreement. Since 2012, our team has completed more than 5,000 project initiatives for the County. From large, enterprise work requests to small, intricate efforts, these efforts, have helped drive County success stories and HPES proudly stands with the County on all of these accomplishments.

All individuals in the project management role are required to obtain certification as a PMP. The standards for certification include both education and experience, and both are required to maintain this certification. Re-certification is obtained through continuing the project management role as well as continued education, volunteer work, and networking.

As an example of our qualifications and experience, HPES currently supports the EPMO for the Next Generation Enterprise Network (NGEN) contract. NGEN represents the continuous evolution of the Department of the Navy's (DON) enterprise networks and will provide secure, net-centric data and services to Navy Marine Corps personnel.

NGEN is the follow-on acquisition approach to providing enterprise network services that were originally consolidated in 2000 under the Navy Marine Corps Intranet (NMCI) contract, which is considered the U.S. government's largest IT outsourcing program, providing IT services to more than 700,000 Navy Marine Corps users. The HPES NGEN EPMO is responsible for the items shown in Figure 17.

Figure 17. HPES NGEN EPMO



We are pleased to create an environment in which the County EPMO and the NGEN EPMO can collaborate and share best practices.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.7.1. Describe your proposed approach to standardize and optimize Project Management practices across a diverse environment such as the County, including, but not limited to, training, tools, standard artifacts, methodologies (including consistency of the methodology across subcontractors that your organization may choose to use), and resource qualifications.

We use the strength of HPES' experience in leading other large programs and the strong relationship we have developed with the County to develop custom processes that meet best practices and County standards, while maintaining communication and alignment between County business groups and HPES portfolios.

The HPES EPMO and County CTO partner are responsible for the integration of these processes across the County enterprise so that service performance can be managed seamlessly. We have aligned our solution to meet County requirements that are the foundation of service delivery, and comply with processes to meet the County's service levels. HPES' EPMO personnel will continue to facilitate the development of processes, manage the deployment, and provide oversight and management for process execution. HPES' EPMO personnel will also establish key roles for ownership and governance of each process, working collaboratively with the County to speed delivery of services focused on quality and adherence to standards.

Internally, the project management team will meet regularly to escalate issues and to discuss project management measurements and trends. They will receive training on updates to client processes, industry best practices, and new tools. We additionally will monitor and meet with subcontractors to make sure

they comply with County and project requirements. We will make certain that subcontractors are aware of and participate in issue and risk management, and that they provide timely accurate status reports.

HPES provides training for project managers, including acceleration programs for the PMP, CAPM, SPI, and other disciplines. Project managers and business analysts are encouraged to join and participate in global, regional, and Community of Practice (CoP) groups, including the USPS PPM Community, the State / Local Government / Education (SLED) Community of Practice, and the USPS Business Analyst Community of Practice, for additional training and shared understanding of best practices across the community.

PMI chapter and PMI/PPM event participation is also encouraged across the organization. HPES partnered with PMI in 2015 Virtual PPM Events. HPES also supports yearly PMI expos and conferences and encourages attendance for education, networking, and PMP certification maintenance.

HPES' PPM Academy provides regular (weekly or more often) opportunities for learning through the Eat and Educate program. Webcasts are provided free of charge, and include topics in Project Management, Risk, Quality, Resources, and other PM Knowledge areas, as well as trends and upcoming changes in PMI certifications.

The EPMO will share in-house opportunities for PM training sessions or vendor sessions, or PM-specific conferences in San Diego, or inform the County that it may participate.

In working with the County, we have identified key standard artifacts that drive project accountability and success. Project management plans play a vital role in setting the proper expectations for the project from beginning to end. They can be much more elaborate for very large, complex infrastructure build-outs or more agile for smaller development projects. Our approach is to leverage the best practice of Project Management Plan development and right-size the project for specific County needs. Project Management Plans will contain one or more of the following sections:

- Scope Statement
- Known Risks and Issues
- Assumptions and Dependencies
- Stakeholder Matrix
- Milestones
- Cost/budget Baselines used in calculating SLs and project success
- All Project Deliverables
- Preliminary Risk Log
- Phased Implementation Approach.

Project schedule templates are maintained in the PPMC. Each framework has one or more templates that meet the needs of their particular project tasks.

The importance of risk management cannot be overstated. Good risk analysis and management plans can keep a project from becoming derailed and unmanageable. Risk analysis and planning is done early in the project life cycle with the help of all stakeholders. Monitoring risk and updating the risk matrix occurs continually during the project life cycle.

Proper change management and communication is also key. For the Applications and Infrastructure frameworks, change management follows the formal change request process that flows through Contracts and is signed by County and an HPES contracts representative.

County-facing project status reports are made available so that authorized County users and HPES Team members can view the status of a particular work request. Status reports for projects are posted on a weekly basis.

All PM work products, status reports, processes, and templates are centrally located/managed and shared using DocVault (described in the tools section).

Each project manager will be responsible for establishing and conducting project meetings with his/her customer.

Third-party vendors working with HPES to implement solutions will be treated as project team members and held to the same process standards required by the County and HPES. From the point of project kickoff, the HPES project manager will be responsible to direct County vendors on their roles and responsibilities for supporting County projects and required deliverables. These responsibilities will include following County-approved methodologies and processes and any project status reporting requirements.

In addition to requiring all vendor project participants to follow County-approved project process, HPES will also identify potential project risks as part of the upfront project risk assessment and will include specific mitigation plans for issues that may arise when operating a project that uses third-party vendors. Those risks will be managed and monitored for risk triggers throughout the project lifecycle.

2.5.7.2. Describe your proposed approach to measuring and analyzing trend data related to the effectiveness and timeliness of Project Management processes and methodologies.

The Project Management Office will work directly with County representatives to recommend and identify the critical performance indices that provide useful project trends and status. Project trends will be calculated and reported on a weekly basis by the Project Management Office and discussed as part of weekly project review meetings. Trends related to project schedule, budget, and other key performance indicators will be monitored on active projects in HPES' Project and Program Management system. If we identify unfavorable trends, we will perform a root-cause analysis to isolate new causes of trends, and provide coaching assistance to project managers to understand the root-cause and provide corrective and preventive action.

The County has designated two critical SLAs around the KPIs of Schedule Performance Index (SPI) and Cost Performance Index (CPI) on Discretionary Standard projects. HPES agrees with the critical nature of these metrics as part of Project Management best practices and supports these KPIs throughout the project lifecycle, measuring progress and reporting on earned value. HPES is constantly managing to these metrics throughout the project lifecycle.

Additional KPIs that HPES recommends based on best practices and the County-specific business requirements include the following:

- KPIs for Project Estimate Accuracy and Response
- KPIs for Impact, Priority, and Mitigation of Risks/Issues
- KPIs for Project Change Management
- KPIs for Projects Opened, Closed, Delivery Times, etc.
- KPIs for Defect Management
- KPIs for Project Schedule Management/Milestone Comparisons

We also recommend continued alignment to identify additional KPIs best suited for the project management organization. The County and the HPES PMO will meet regularly to discuss overall objectives, issues, and improvement items, which can be incorporated into ongoing KPI development and improvements.

Because HPES understands the importance of project estimating, the Project Management Office will provide tools to collect and measure the effectiveness of estimates against actuals for all standard projects from initiation to closure. We will review trend reports monthly, along with individual reporting per

project. The data collected will include estimates at initiation, actuals by role at closure, total project CPI/SPI, number and type of change requests, and cost impacts. We will also collect data to determine the effectiveness of ROM estimates for project management and engineering project activities and continuously update the Basis of Estimate process and provide more accurate and predictable ROM estimates.

2.5.7.3. Describe your organization's proposed approach to the relationship between project managers and Service Framework resources, including the process for how project managers engage needed resources from Service Frameworks for various project activities without compromising either project timelines or Operational Services.

Our current processes identify the right mix of resources from all Service Frameworks for project success. Where possible the same project resources engaged for creating project ROM estimates will also be responsible for delivering the end product. This approach drives a high level of accountability and quality for our solutions.

Starting with the project's initial estimate, we will engage the solution frameworks to provide rough estimates for the project's proposal. Once a project is approved by the County, we will initiate an internal kickoff with the team, and the project manager will engage the framework leads to determine the level of resources and effort needed from the initial requirements gathering through deployment. Requirements Development and Planning will engage the framework resources to refine the solution and further refine the estimate of resources needed to deliver. During execution, testing, and deployment, the various frameworks will be actively engaged in providing and testing the solution, and positioning for, executing, and supporting deployment. At project closure, the framework resources will continue their involvement to make certain that warranty-period support is available, turnover to production is successful, and project close-down ends with a final collection of effort and lessons learned. These touchpoints are embedded in the standard project plan templates and reflected in the project management life cycle.

Throughout this processes, we will identify framework SMEs from operational support when needed to advise and provide critical product information and input to the project team while supporting the operational needs of the product.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

Integration and Testing Services (Sched 4.3, Section 2.10)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Software defects can cause system outages that could impact the County's operations and affect the County's critical applications. HPES has a comprehensive testing framework that includes the structure, processes, tools, and templates to enable consistent, high-quality testing services and deliverables. Our testing framework verifies compliance with the application development process and validates the quality of the application to address the commitments outlined in the SOW. We achieve maximum integration testing efficiency by grouping testers separately from developers.

Testing success relies on a comprehensive strategy that defines an overall testing approach. To provide guidance and establish a framework for defining, planning, executing, and managing all testing activities, we will first work with the County to determine the level of strategy that best meets its needs. We will review the current strategies, testing requirements, business needs, and priorities to develop the most efficient and cost-effective testing strategy for the SOW project.

Our approach to developing the testing strategy is to supplement and support the project life cycle with the following testing-specific information:

- Testing roles and responsibilities
- Testing methodology
- Test levels to be performed
- Test coverage to be performed for each test level
- Test deliverables
- Test management and measurement approach
- Required testing environments and tools.

Testing activities require planning and management to fully succeed. Based on the priorities identified in the test strategy, we will develop a Test Plan that covers each required test level and provides tactical guidance by specifying the following factors:

- **Test Scope** – Scope of HPES' testing services to be provided, including test types
- **Test Schedule** – Schedule for all phases of testing, integrated with the overall project schedule (test development, test execution, testing metrics collection, and testing reporting)
- **Test Roles and Responsibilities** – Test roles/responsibilities for all participants, including the HPES team, State staff, and third-party vendor staff; responsibility for test environments and tools
- **Test Design/Methodology** – Test case design techniques/strategy for each test level
- **Test Procedure/Execution** – Test-level execution tasks, including participants, to conduct execution; entry, exit, pass/fail, suspension, and resumption criteria for each test level
- **Test Tracking and Reporting** – Test results data collection requirements, documentation, and reporting; test progression tracking and error/deficiency management/resolution process; risks specific to a test level that require mitigation.

The HPES Test Plan also outlines the recommended testing tools and testing management and measurement.

A critical part of the test plan is testing management and measurement to make sure that testing meets the project requirements. HPES applies and adapts the processes, techniques, and templates of our testing method to effectively manage and control the planning, execution, and completion of all testing activities. Testing management and measurement involves the following actions:

- Establishing and maintaining detailed estimates, a test schedule, resource plans, and procedures for all testing phases
- Managing preparation of test plans, scenarios, and test cases for each test level
- Establishing acceptance criteria
- Managing the execution of test cases, tracking and resolving defects, and verifying completion of tests, including regression testing
- Managing testing close-down, including reporting.

To make sure the application is ready to move into production, HPES applies comprehensive metrics, supported by standard testing management tools. We generate reports to provide insight into the status of testing throughout the project. With this information, we confirm that tests are mitigating risks on high-priority requirements. These metrics support timely corrective action and informed decision-making by all project stakeholders, particularly "go/no-go" decisions to progress through project phases.

System testing involves testing both an application and its supporting infrastructure. HPES provides system testing to establish confidence that users will accept the system and that the system is functionally and structurally stable, reliable, secure, and interoperable. System testing encompasses an integrated system or a logical subset of application functions the system will deliver. It verifies compliance with

functional and nonfunctional system requirements and specifications. The process normally involves creating test conditions for evaluating the application and its infrastructure.

We prepare and perform system tests based on approved requirements documents, the application architecture, and the application design specified by the development team. We create tests to exercise the specific business functions selected and submit them for County approval. This approach helps to validate that the system performs according to the County's requirements.

System testing includes testing interfaces with external entities and with batch and online software. All parts of the system must be available for system testing to succeed. Data enters through normal interfaces so we can test interaction between various subsystems. If the County does not have an appropriate testing environment available to accept transactions or files, we may use emulators to simulate interactions with external systems. System test activities include the following:

- Test cases, standard and ad hoc
- Test data management
- Requirements Traceability Matrix (RTM)
- Performance benchmarks when applicable
- Summary report.

We use automated life cycle management (ALM) tools and techniques as we develop system test cases based on functions and roles. Function-based tests validate the application's functional requirements and data flows. Role-based tests verify access to the application, menus, submenus, buttons, and icons; verify a complete and correct process flow for each defined role; and validate that access covers only specified areas.

Table 12 describes our high-level input criteria, activities, and deliverables for test cases.

Table 12. HPES Test Criteria and Deliverables

INPUT CRITERIA	• Baselined test scope, strategy, and plan • Baselined effort estimation and schedule • Baselined defect, change, configuration, communication plan, and risk management plan • Baselined and updated Trace Testability Matrix (TTM) Baselined design, business requirements/specifications, and use cases documents
ACTIVITIES	• Identify functional and technical test scenarios • Update affected test case and script • Design new test cases and scripts: review, sign off, and baseline • Define success criteria and expected outcomes • Design test data: review, sign off, and baseline • Collect metrics Update test traceability, arrive at test coverage, and sign off
DELIVERABLES	• Baselined test cases, scripts, and test data • Baselined smoke test suite • Baselined test traceability Sign-off by stakeholder

Test data management plays a central role in testing. From the lowest level (method tests) to the highest level (acceptance tests), a test involves input data, expected output data, and a comparison between expected and actual output data. There are several advantages to separating test data from test code:

- Test data can be edited, making it easy to add test cases.
- Test data can be validated as a means of reducing "false failures"
- Test data can be externally generated or captured from a production process.

There are several approaches to test data management; HPES recommends the database approach. With databases, we can access and analyze data easily; they also simplify report generation. The database offers the most flexibility for comparing data taken from different tests, test stations, or even geographical locations. Databases are more maintainable than the other options, complete with built-in archiving capabilities. The main reason to use a database approach is that data storage and retrieval details are separated from application-specific complexities.

The RTM traces downstream work products of the requirements, such as design, code, and test cases. If an RTM exists, our testing team updates it when the initial test design is complete, to map requirements to test cases. If an RTM was not developed, we establish one while developing test cases, linking each test case back to the original requirement.

Next, as we execute test cases, we document and map any defects we encounter to the corresponding requirements in the matrix. The updated matrix provides a running record of how testing has addressed and met each requirement, revealing gaps the testing team needs to fill and opportunities to consolidate redundant tests.

The County will receive a complete overview of system testing results in a system test summary report, which includes an overview of the approach, tools, test cases, activities, results, and any outstanding defects.

System integration testing confirms that the necessary communications and setup exist to perform functional testing and addresses the need to assess whether the system interfaces smoothly with other applications or systems.

After the development team provides the testing team with the interface code, we perform system integration testing. This testing is often the most complex because it normally involves communication and security layers and requires coordination with outside organizations.

Certain applications may involve providers external to the individual SOW. When testing with an external organization, we provide that group a copy of all test cases to review to support test coordination and data synchronization. To support external interface testing, we work closely with the State project manager to coordinate and cooperate with third-party interface owners.

Our goals in performance testing are to: 1) understand the performance requirements; 2) determine the types of performance tests and the test volumes that best meet those requirements; 3) test the system performance; and 4) ensure the new change does not impact existing functions or systems. We also assist the County with performance tuning recommendations to help fix performance-related issues. Our methodology includes the following actions:

- Identify and scope requirements
  - Performance test requirement analysis, review of volume metrics and performance goals
  - Performance test strategy and planning
  - Arrive at scope effort, cost, and timeline
- Determine performance testing type
  - Load testing

  - Stress testing
  - Volume testing
  - Scalability
  - Failover testing
  - Regression testing
- Review and provide recommendations of performance test scenarios and volume metrics performance goals provided by the project team
- Develop performance test strategy, test plan, and scripting standards
- Set up and maintain the test environment, including build and deployment activities
- Prepare test data for project owner's review before baseline
- Design, execute, and analyze performance test for approximately four performance test scenarios identified and provided by the project team
- Provide required support for the performance tuning team, such as re-execution of scripts to identify replicating issues.

Table 13 presents our detailed performance and load-test strategy.

Table 13. HPES Performance Testing

PHASE	INPUT/ENTRY CRITERIA	ACTIVITIES	DELIVERABLES
Discovery Phase (Requirements Analysis and Performance Test Planning)	• Application non-functional requirement specifications (SRS, design specifications, and so forth) • Business scenarios, performance test scenarios, use cases • Performance goals and volume metrics • Release scope • Production environment details	• Conduct requirements study • Determine test scenarios and impact analysis • Identify test scenarios for performance testing • Develop performance test strategy/plan • Derive test environment specifications • Conduct performance test scenarios, test strategy/ plan, traceability, review, and approval	• Performance test strategy/plan • Identified test scenarios for performance testing
Performance Test Environment Preparation/ Readiness	• Performance test strategy, plan • Tools and licenses • Application builds • Performance test environment • Functional test cases • Performance test scenarios, test cases and test data, sample test data • SRS, design, other specifications	• Set up and configure test environment • Deploy and configure application build • Identify performance testing tools, monitors, installation, and setup/configuration • Test data preparation, review, and baseline • Test environment and build validation through sanity testing	• Performance test environment with latest build • Performance test data • Performance test tools installed and configured
Performance Test Design/ Development	• Performance test scenarios • Identified performance business scenarios • Performance test plan	• Develop performance test scripting standard • Develop performance test framework	• Performance test framework/ harness • Baseline performance test

PHASE	INPUT/ENTRY CRITERIA	ACTIVITIES	DELIVERABLES
	• Test environment with latest stable build • Performance test data • Performance test tools installed and configured • Baselined performance business and test scenarios	• Develop test scripts/test suite (integration of test scripts) • Develop test data files • Identify and review performance test metrics • Review and baseline all above test artifacts	scripts and test suite(s) and associated test data and configuration files
Performance Test Execution, Analysis, and Reporting	• Performance test strategy and test plan • Test environment with latest stable build deployed • Baseline test scripts • Non-functional requirements (performance goals and volume metrics) • Test environment sanity test and all test entry criteria	• Validate test entry criteria • Execute performance test • Validate test exit criteria • Analyze and report performance test results • Collect performance test metrics • Log and track defects	• Performance test execution status reports • Performance test results, performance issues, bottlenecks, metrics reports • Sign-off report
Performance Tuning Support and Post-Tuning Testing	• Performance test results and reports • Performance test results analysis report and recommendations for tuning • Performance goals and volume metrics • Test entry/exit criteria	• Validate test entry/exit criteria • Provide performance-tuning support • Provide post-tuning retesting of scripts • Conduct result analysis of post-tuning tests • Provide performance test reporting for post-tuning tests	• Post-tuning test results • Post-tuning performance test reports • Final sign-off on performance test report

To identify and correct vulnerabilities before the application goes into production, HPES provides Security Testing Services, which make sure the County's applications are protected against exposure to hackers or other threats to their integrity, availability, or confidentiality. Security Testing Services can help the County achieve the following goals:

- Improve coding and security practices
- Identify and eliminate or mitigate security vulnerabilities in web applications
- Comply with regulatory and reporting requirements
- Test existing applications and quickly address major vulnerabilities
- Cut overall project costs by identifying problems early.

Applications require varying levels of security testing depending on the purpose, the customer base, and the data contained within the application database. To address security risk levels associated with unique applications, we offer vulnerability code scanning and application security testing. We will work with the County to assess the application risk level, then recommend the types of security testing required.

We recommend vulnerability code scanning for medium-security-risk applications. First, we scan the code to identify critical vulnerabilities, then we assist the development team with remediating issues and applying regression testing code fixes to address these vulnerabilities.

We recommend application security testing in the testing environment for high-risk web applications to uncover security vulnerabilities before moving the application into the production environment. We will

assist the development team with remediation and regression testing of code fixes to address the vulnerabilities uncovered.

Regression testing involves selectively retesting previously tested functions and running selected test cases to make sure that new development and defect fixes have not introduced or revealed new faults. Regression testing can occur throughout testing and must be executed whenever the build changes. It occurs at all test levels of our Enterprise Testing Methodology and throughout development.

During test case development, HPES identifies candidates for regression testing. Typically, we select those cases that test the correct workings of the critical system components and functions. We can then use these cases to test future application releases. The following changes typically require regression testing:

- Addition of new business functionality (new modules or sub modules, new business transactions, new business processes)
- Modifications to current functionality (enhancements, defect fixes) for a release
- Implementation of the current application to new locations
- Upgrades to more recent versions of the application or operating system
- Hardware upgrades.

Business regression testing focuses on the critical, high-volume business processes for all business functions introduced up to or including the previous software release. Our approach is to build on previous regression tests by adding new scripts with tests based on the last release's functions. We focus specifically on known high-risk areas.

HPES may also perform regression testing after completing a major type of testing (such as system testing) but before releasing the application to the next test level. In this way, we verify that all required defect remediation has been applied and that new and previous functions work correctly.

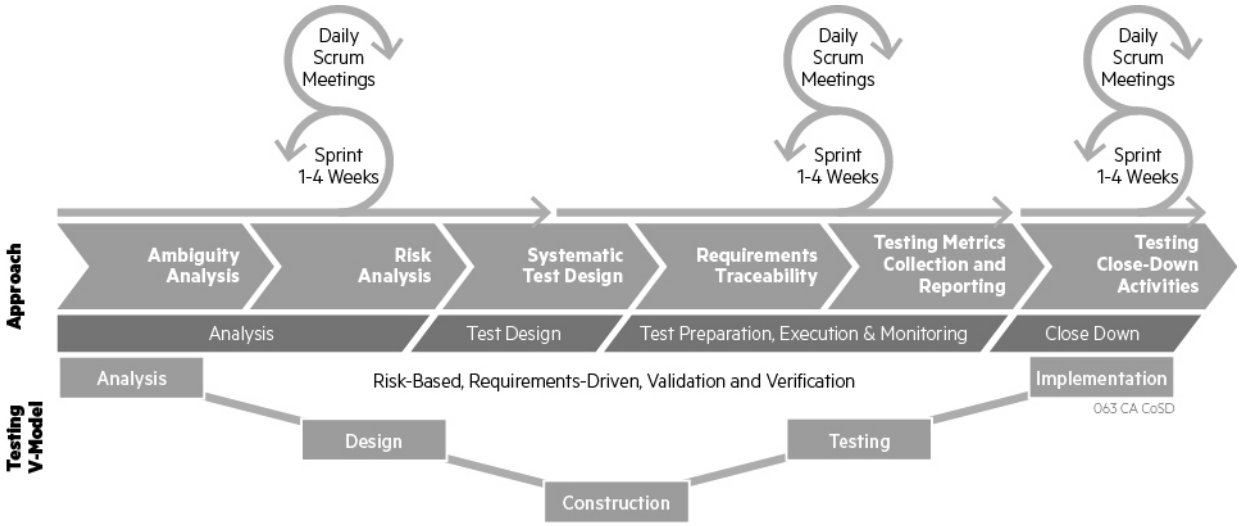
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES facilities in Ranch Bernardo, CA; El Paso, TX; Pontiac, MI, depending on skillset required.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES' testing methodology is shown in Figure 18. The HPES methodology aligns with the industry-accepted Testing V-Model.

Figure 18. HPES' Enterprise Testing Methodology



Our testing and quality assurance approach focuses on individual SOW requirements, minimizing risk and increasing the value of County applications with high-quality, consistent testing that complies with the County's development and delivery processes.

Our risk-based, requirements-driven testing approach includes the following components:

- **Ambiguity Analysis** – While performing requirements validation, we systematically analyze ambiguities in the requirements that drive application design, development, and testing to minimize inconsistencies and maximize clarity. This process helps to meet users' expectations; gives the project team a targeted and complete plan; and builds common understanding of requirements for project managers, developers, testers, and users.
- **Risk Analysis** – Risk-based testing focuses on analyzing risks to reduce misdirected or incomplete test coverage. We systematically analyze requirements to determine the priorities that guide the testing strategy. All stakeholders, including third-party interface owners, are engaged in these analyses. We define test environment requirements early in the life cycle.
- **Systematic Test Design** – Through methodical activities focused on managing and mitigating risks, we apply test design techniques to plan, choose, and develop the most effective tests to deliver the required amount of testing.
- **Requirements Traceability** – Throughout test development and execution, we update the RTM to comprehensively depict test coverage and to keep testing focused on high-risk, high-priority requirements. Because each test case inherits priority from its requirement, the RTM helps the team analyze the testing impact of any requirements changes.
- **Testing Metrics Collection/Reporting** – We use testing reports to gain ongoing insight into the progress of tests and defect resolution, and we offer timely opportunities for mitigation of a risk before it causes harm to the State's environment – or to the application itself.
- **Testing Close-Down Activities** – Ideally, testing ends with all tests executed, all defects resolved, and a system unquestionably ready for release. We focus on satisfying high-risk, high-priority functionality first through risk-based testing, leaving as the last priority tests and defects for only low-risk, low-priority requirements as agreed to by the State. As part of project close-down, we can either transition the work to the State, as outlined in the SOW, or continue providing maintenance and support.

- Automated Tools – Automated systems and tools involved in proposed solution

Our testing professionals have experience with a variety of testing tools; however, our preferred testing tool set is HP Application Lifecycle Management (ALM). As an industry leader, HPES provides an integrated tool set which manages test cases, provides requirements management, and integrates with many change management/ release management tools. The HPES tool suite includes the items shown in Table 14.

Table 14. HPES Integration Testing Tools

TESTING ACTIVITY	HP TESTING TOOLS
Quality Management	HP Application Lifecycle Management (ALM)/Quality Center
Testing Management and Measurement	
• Perform functional testing • Manage testing • Move test cases and test scripts and track test results for all test levels to repository	
Requirements Validation	HP Requirements Ambiguity Checker
Performance Testing	HP Performance Center
Regression Testing	HP Unified Functional Tester

- Qualifications and Experience – Background and experience in comparable environments

Solution Description

HPES provides a global solution for managing projects and programs at Global Oil Production Company. Project managers are supported by Program Management Office teams across EMEA, America, and Asia Pacific. The group has end-to-end accountability for all programs and projects across the client account, including new business, transformation, and release management so that all projects and programs meet scope, time, budget, and quality expectations.

HPES manages approximately one-third of the client's 1,500 yearly infrastructure projects - about 500+ projects a year. HPE provides a Global Project and Program Delivery (GPPD) organization composed of 200+ dedicated project resources to manage the following:

- More than 300 concurrent projects globally
- New service development, service delivery, and strategic programs
- Project initiation, project delivery, and project monitoring and control through an integrated delivery and quality assurance approach managed by the Program Management Office
- Leveraged and non-client account PPM resources

Scope

- Proposal/request management
- Project initiation
- Project execution
- Project monitoring and control, including delivery and quality assurance and customer service levels (CSLs) compliance
- Handover to operational support

- Demand and resource management for project managers, technical architects, engineers, and business analysts
- Continuous improvement, communication, and training

Customer Service Levels

- Project initiation
- Compliance with project management methodology
- Compliance with project reporting
- On time/on budget
- Customer satisfaction scores
- Execution of multi-bundle projects

Capacities/Volumes

- 500+ projects per year

Client Benefits

CXO Business Benefits

- Project-by-project benefit defined for more than 500 projects per year
- Minimized risk of change associated with approximately $50M in project spending

IT Metrics

- Enable improved IT services
  - Input to Continuous Improvement
  - Influencing Speed to Deliver
  - Input to quality processes
- Leveraging best practices appended by specific tools and processes
  - Supporting internal project governance
  - Certifying compliance with processes and tracking CSLs
  - Conducting joint health checks with client PMO on client key projects

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.8 Incident Management (Sched 4.3, Section 2.11)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

As the current provider for the County, HPES understands that an effective incident management (IM) process and team is key to identifying, analyzing, correcting issues/incidents, and preventing their reoccurrence. We have in-place a highly skilled team of incident managers who work with the various SMEs, vendors, and the County to restore services quickly to end users. This team has a vast level of experience and expertise when it comes to the County's users and their business, applications, and infrastructure.

As a part of this process, all incidents receive prioritized attention, depending on severity, Service Level Agreement (SLA), or the immediate service restoration needs of the County. Without an effective process and team, an incident can rapidly disrupt business operations, information security, IT systems, employees, the public, and other vital County functions.

Solution: HPES has a proven IM process that includes ITIL methodology, which is widely used by our professionals and has been further developed and improved in collaboration with the County. We will continue to improve this process based on needs and other requirements. During the transition period, this process will be used as it is today.

Our focus remains:

- Restoration of service operations as quickly as possible using repeatable streamlined processes and escalation points
- Frequent, clear, and concise communications to end users and CTO through resolution
- Minimizing the adverse impact of incidents on the business
- Providing departments and end users with a single point of contact (POC) for all incidents reported
- Maintaining portal-based visibility into incidents and trouble tickets with drill down to detailed information.

HPES provides full life cycle IM through our service desk and IM functions. Our objective is always to restore normal service operations as quickly as possible and minimize the adverse impact on County business operations. To accomplish this, the HPES service desk will act as the initial POC for the identification, categorization, and tracking of all County incidents in our service management system. This system will provide the efficient assignment of incidents for resolution by the responsible teams and direct access to incident status by County personnel. The system will also objectively measure accountability for all aspects of the IM process.

Rationale: HPES has IM expertise and experience, having evolved this practice into our common service management platform and on other HPES IT management contracts. Moreover, our intimate familiarity with County needs and history enables us to continue to provide this service with no disruption in current processing and informs and validates our technical solution. The IM team consistently achieves high customer satisfaction scores in surveys with CTO and end users.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Incident management will be supported by the following groups:

- Service Desk
- Service Delivery Managers
- Applications SMEs
- Datacenter SMEs (network, storage, exchange, BUR)
- Local account server team/Infrastructure SMEs
- Desktop and Remote Support Technicians, as needed
- AT&T
- Engineering and Architecture

The majority of the services provided by this process will be supported by the account team at HPES' Rancho Bernardo site; AT&T will provide services from Trade Street.

Datacenter and other areas supported by leveraged frameworks will remain as they are in place today with supplemental support provided by the account team in Rancho Bernardo. The Service Desk will provide support from Pontiac, MI.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

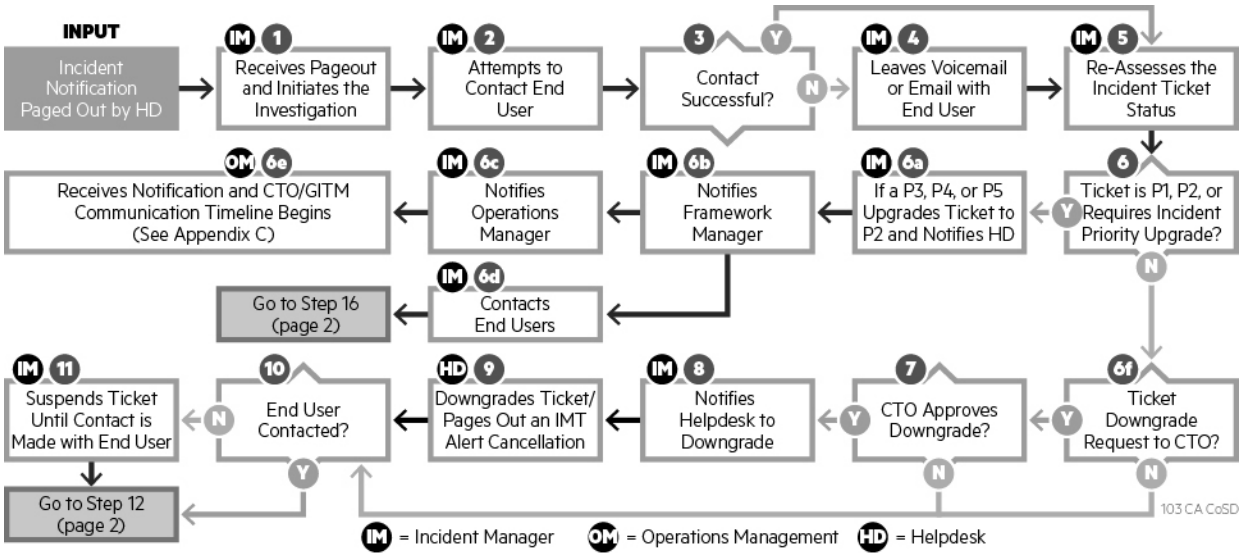
HPES will continue to provide full life cycle IM using our existing processes as stated above and described in detail below. One major change going forward will be the addition of SDMs as key positions in the Contract. Each SDM will be assigned to a County business group and led by the enterprise SDM. The main objective of this role as it relates to IM will be to restore normal service operation as quickly as possible for the incidents impacting their Business Group while minimizing the adverse impact on County business operations. The HPES service desk will serve as the primary point of contact and owner for the identification, categorization, monitoring, and tracking of all County incidents within our service management system, providing efficient assignment of incidents for resolution by responsible resolver teams and direct access to incident status by County personnel. The system will also objectively measure accountability for all aspects of the IM process.

The HPES service delivery management team will continually monitor incidents, responses, escalations, and resolution activities through the ticketing system for compliance with procedures and performance objectives. The HPES SDM will provide key configuration items (CI) for incident components. During major (high severity/scope) incidents, the SDM team will actively facilitate status notifications and escalations to all appropriate levels in customer and vendor organizations. Our approach will provide the right people, processes, and tools to perform comprehensive IM for the County, who will receive timely responses to questions and issues as they occur and progress through the incident life cycle.

The HPES service desk and service delivery management team will continue to refine a mature process for full life cycle IM while including the processes and procedures we have in place today. Each sub-process and step is described in Figure 19. This process assigns Level 1 support responsibility to the HPES service desk, which is also responsible for incident recording, categorization, and assignment. The enterprise SDM will act as an escalation point and operations orchestrator, helping the County achieve continued high levels of service and user satisfaction.

The HPES enterprise SDM will be responsible for verifying prioritization and categorization standards for IM processes in collaboration with the County, validating that we record these standards in the policies and procedures and continuously monitor other service providers' compliance with these standards. The team will also be responsible for verifying procedures and mechanisms for handling, expediting, and communications of high-priority incidents. These procedures and mechanisms will be recorded in the Service Management Manual and also be continually monitored for compliance.

Figure 19. Incident Management Flowchart



*Today, we work to support the County's mature process for full life cycle IM that provides the right people, processes, and tools for comprehensive management. *Note - This diagram is an excerpt from the County's current process documentation.*

The HPES SDMs will continually monitor and review incidents within the ticketing system for completeness, accuracy, proper categorization, and timeliness of resolution activities as established by the County and HPES and defined within the policies and procedures within their respective business groups. Each SDM will provide operational data and information related to outages and issues, among others, for their respective Business Group. The SDM will, on a weekly basis, provide reporting of this review to the County Technology Office, operational POCs during the existing weekly Operations status meeting.

HPES will continue to document and provide procedures for enhancements related to incident resolution. Scripts, techniques, and step-by-step actions will be recorded in the knowledge management system, subject to change management processes, for future use by support personnel and user access for self-help.

Our IM process will assign initial responsibility for the identification of problems to the resolving service providers in the problem management process description. If an incident is the result of a change, we will record the information and refer it to the change management process. If we determine an incident qualifies as a problem, we will record it in the incident record for referral to the problem management process. HPES' SDMs will be responsible for IM and problem management for the business group, and will verify evaluations performed in this step and escalate incidents to the change and/or problem management process as required.

SDMs are responsible for monitoring and managing the entire life cycle of incidents to comply with resolution, status, and notification processes as well as procedure requirements of the service desk. As part of our performance-based management approach to quality assurance, we will actively monitor and remediate underperforming KPIs and incorporate them into our continuous improvement process. We will prepare a quarterly action plan to address service improvement objectives and activities for County review and implementation approval.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES' primary tool for IM is HPE Service Manager Enterprise Suite, a comprehensive, fully integrated ITSM solution that leverages more than 25 years of service management focus and experience. It provides a powerful platform to standardize, automate, and enforce key IT processes and demonstrate value to our customers. It offers efficiencies through automation of core IT processes such as incident, problem, service level, and end-to-end change and configuration management. The suite orchestrates ITSM processes and enables customers and vendors to track calls, requests, incidents, problems, changes, releases, configurations, and SLAs. Approved vendors will have the ability to use this system as they use the current system today (see list below for current vendors with access) and additional vendors can be added as approved in the future..

Vendor List:

- AT&T
- WAVE
- LMS

- Qualifications and Experience – Background and experience in comparable environments

HPES is eminently qualified to provide IM support to the County. Examples of our qualifications and experience include providing the following services to NGEN, HUD, and City of Anaheim:

- 300+ ISO/IEC 20000 certified professionals
- More than 20,000 people ITIL certified
- 1,100 ITSM delivery professionals worldwide, managing service quality to our clients
- Processes, filters, and manages more than 1.5 million service incidents and alerts per month
- Logs and manages approximately 4.4 million calls, incidents, changes, and requests monthly
- ITSM platform, standard reference architecture (SRA), is deployed for more than 500 clients worldwide.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.8.1. Describe your proposed approach to staff and respond to Priority 1 Incidents.

As documented in the County Standards and Procedures (CoSD-175), when a Priority 1 incident is received, it is logged into Service Manager and an electronic alert is sent out along with an eNote page to the appropriate support staff. The SDM on point receives the page with the incident ticket number and immediately ensures the frameworks are engaged and have begun work on the issue and preps for customer notification. If services cannot be restored within 30 minutes a bridge line is stood up with all frameworks on the call until resolution of the issue. The SDM sends the first status to the County user and CTO within 60 minutes and the status continues every hour until service is restored.

The SDM will monitor and track the incident ticket to closure and provide all required status communications during the incident life cycle. When a change in the status of the request occurs, the SDM determines if the ticket issues have been resolved or if the status change is valid. If issues have not been resolved, the SDM continues to monitor and track the request until resolution.

If the ticket issues have been resolved, the SDM sends out final communication and status and proceeds with next steps based on ticket priority. If the ticket is Priority 1 or 2, the SDM makes sure that an RCA has been created. When the problem ticket has been completed for Priority 1 or 2 issues or a permanent

solution has been implemented for non-Priority 1 or 2 issues, the SDM documents all the actions taken in the activity fields of the ticket and changes the ticket status to Resolved.

2.5.8.2. Describe your proposed approach for trend analysis of Incidents to identify and correct recurring Incidents.

The HPES enterprise problem manager will be responsible for analyzing quality and reporting trends related to incidents. This analysis will provide recommendations of appropriate actions to mitigate any negative findings and to propose improvements to drive improved effectiveness and efficiency. As part of the analysis, once a trend is identified, action can be taken to correct, improve the outcome, or prevent future outages from occurring. These reports will be provided on a periodic basis. Our proactive method includes performance-based management and periodic assessments of HPES KPIs within the IM framework and will include capturing underperforming mission-critical KPI and SLA metrics, escalating them as necessary, and displaying them on the EPMO status dashboard. We will also use this data to identify and substantiate trends relating to similar incidents or contributing to problem recurrence, and developing solutions to address chronic issues. An integral part of our continuous improvement process, we continually assess these indicators to identify negative trends. We will continue to conduct RCAs where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends; thereby ensuring year-to-year continuous improvement.

2.5.8.3. Describe your proposed approach, in detail, for RCAs, include tracking of RCA remediation items to ensure appropriate and timely resolution.

HPES will leverage our current experience performing problem management activities in support of IM, change management, and release management to identify and resolve the underlying root causes of problems. We will use RCAs to determine the cause of an incident, identify appropriate problem resolutions, document findings, and provide recommendations to prevent recurrence of the problems. In addition to the Six Sigma "5 Whys" approach to root-cause determinations, which is described in Proposal Section 2.5.9, the following details our RCA approach:

- Once Priority 1 and Priority 2 incidents are resolved, the RCA manager will determine if an RCA is necessary. If required, or when the RCA manager receives a request from the County, the RCA manager will enter information into an RCA Submittal Form and submit it to the appropriate SME and framework manager.
- Once received, the SME will:
  - Gather additional data from other framework SMEs as needed
  - Determine the chronology of events and causes
  - Determine any underlying root and contributing causes and how they manifest
  - Complete the RCA and develop corrective action items/recommendations
  - Complete the RCA Submittal Form and submit findings for Peer and Tower Management Review
  - Once the SME findings have passed Peer and Tower Management Review, the SME submits the findings to the RCA manager
- After receiving the findings, the RCA manager will schedule a formal review by the HPES RCA team.
- The team will then determine if the RCA is complete and, if so, will address all concerns. The RCA manager will conduct a final Quality Review and submit it to the RCA team for their final review. On final approval, the RCA will be submitted to the CTO RCA representative for final disposition.
- This process will be completed within 6 business days of the final resolution of an incident ticket or receipt of an ad hoc RCA request from the CTO.
- For RCAs related to an outage that is business group specific, the SDM make sure all required information is gathered and provided.

Corrective action items that are not completed as a part of the incident resolution in the RCA are documented in the Problem Management SharePoint site with an owner and date of completion assigned. This system has automatic email alerting assigned to it for the POC to make sure items are completed as required. The Enterprise Problem Manager is responsible for validating and verifying that all items are completed on the site within the timeframe that is documented. The HPSM (HPE Service Manager) system will provide a problem case number for all corrective action items and problems being worked that do or do not have a RCA as a requirement. These Problem cases will make sure that we have complete tracking and a connection between the incident and the change records required to act on the items that need to be addressed. These cases will not be closed until all activities are completed and documented.

Additional clarification and details of this process can be found in the RCA process documents COSD-159, COSD-160, COSD-161, and COSD-162.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.9 Problem Management Services (Sched 4.3, Section 2.12)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES is a recognized industry leader in IT service management, particularly as relates to incident and problem management and in accordance with ITIL guidelines and globally implemented best practices. Our methodology, combined with our years of experience and relationship with the County, is what we use today to solve systemic or chronic issues in the environment. Problems requiring management and resolution typically arise as a result of one or more similar incidents or through proactive trending data that is reviewed by the enterprise problem manager. The ability to manage problems in a repeatable and methodical manner helps to minimize disruptions to the County's IT services, prevents recurrences, and is a hallmark of HPES' overall service delivery management model. The practices that are in place today will continue in the subsequent Contract and will be modified and improved on an ongoing basis in collaboration with the County.

Problem management may require the investigation of root causes to memorialize occurrences in our knowledge repository and eliminate future occurrences wherever possible. The process also makes sure that corrective actions and resolutions are implemented through the appropriate control procedures, such as change and release management. Active incidents and problems will be documented at every step and the status will be accessible for end-user review through the Service Portal.

As we have in place today, problem management systems will also maintain information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number and impact of incidents over time. Although incident management (IM) and problem management are separate processes, they are closely related and will typically use many of the same tools and data points. This will help with effective communication and documentation when dealing with related incidents and problems.

Solution: In addition to the existing processes and support resources that we have in place today, a key element of our approach is assigning a single service delivery manager (SDM) per business group to act as a single point of escalation and communication. This service has been proven valuable, as it removes the question of "who do I contact?" when issues are being worked and makes sure that the focus remains on the resolution of systemic issues. Moving forward, we will take steps that further enhance the ITIL

framework, putting and more formalization around this process in an effort to continue improvement and to maintain environmental stability.

Problem management is under the purview and responsibility of SDMs who will make sure that all problems are resolved, including root cause determination when necessary. They will additionally make certain that all problem-related activities be reported and recorded, archived, and made available to County stakeholders.

Rationale: HPES has a well-documented proven problem management process in place that has led to the resolution of many issues in the County's IT environment such as:

- Outlook disconnects
- Latency reports at sites 55, 34, 270, and 277
- Repeat AD account lockouts
- Symantec AV client update issues.

As a part of the process, we take a hands-on approach with the County during the resolution of these issues and facilitate consistent and clear communication until resolution. Our SDMs will be responsible for understanding the problems and how they impact their business group and make sure that proper communication and discussions for that group takes place and that resources are available to support the resolution and recording of IT problems.

Problem management will be a daily responsibility for the SDMs and they will be assigned activities to work—whether it be proactively or through tickets, escalations, or other similar activities. HPES has an enterprise problem manager who will report, track, and communicate all problem management issues worked by the team and the account via the weekly CTO operations status meeting.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The majority of the services provided by this process will be supported by the account team at HPES' Rancho Bernardo site.

Data center and other areas supported by leveraged frameworks will provide supplemental support.

The Service Desk will provide support from the Pontiac, MI facility.

AT&T will provide services from Trade Street.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

For HPES, a problem is any event that has the potential to inhibit the County's ability to perform a business function. This is a common understanding and best practice between HPES and the County today, as we jointly understand the importance to successfully recognize and remediate problems quickly. We have well-defined processes, key performance indicators, and mature IT tools to alert our integrated delivery teams when conditions indicate the potential for a problem to occur. Our main goal is to minimize or prevent service degradation to the County's end so they can continue to perform their duties and service the public unimpeded. We will train all program team members of these processes, best practices, and lessons learned are shared to maximize effectiveness, promote reuse of knowledge, and optimize project timelines.

Problem Management Techniques and Controls

As discussed in other sections of the proposal response, standardization is a primary success factor. HPES will continue to enforce a standard "plan, do, measure, adjust" methodology to continuously recognize, react to, and correct problems quickly. Team members are trained to report all issues to the appropriate SDM or enterprise problem manager, who will identify the owner responsible for resolution. If the owner fails to resolve the issue within a specified time frame, the SDM will initiate our predefined escalation process to prioritize and broaden the focus on resolving the problem. Any individual, County, or HPES employee, may identify a problem although they usually originate as incidents or changes. As a standard practice, we conduct enterprise-level delivery reviews weekly to share experiences across the IT services and cross-functional frameworks to identify and mitigate risks. These efforts and practices have contributed to successful communication of the issues being worked as well as the resolution of issues. Relevant examples include Outlook disconnects, antivirus pushes, and site latency.

"Another thing that differentiates HP and why I do recommend them so frequently to current and past colleagues is their ability to execute in a highly dynamic operational environment. My world is turbulent with lots of change and inherent conflict. HP understands this and comes to the table prepared to engage with this turbulence. Further, HP does really well engaging in situations (without direct oversight in many cases) where there's conflict in the air. They are able to consistently minimize that conflict and do it in a way that preserves and promotes positive relationships. On a day-to-day basis they're able to adapt and change their trajectory/execution profile based on what the Federal Government is doing that particular day, week, or month. That's a really hard thing to do. I haven't found too many contractors that are able to do that, especially in a fixed firm price contractual agreement."

— Aaron Lindstrom
VA Program Manager
and COR

Recognizing Problems - HPES uses a methodology-based approach to recognize, address, and correct problems that may arise throughout the IT organization. Our approach combines proven problem management methods and processes, such as root cause analysis, with open communications, transparency, and continuous/iterative feedback. We will proactively analyze, measure (through leading indicator KPIs), and monitor performance through these multiple channels to increase the probability of identifying and mitigating risks and issues early, before they manifest as incidents or problems.

Correcting Problems – The applicable SDM will oversee corrective investigations and problem remediation by designated support representatives. They will use incident or trouble ticket input as well as procedure manuals, knowledge databases, and other tools to resolve the problem. The SDM will determine if a workaround can be provided or identify a permanent solution to the problem. Once a workaround or permanent solution is determined, the SDM will decide on the change needed to implement the workaround or solution. If a Request for Change (RFC) is required, the SDM will create an RFC using CHG 1.0 RFC. If an RFC is not needed, or after the RFC has been approved, the SDM will determine whether the implementation of the workaround or solution requires infrastructure support. If needed, the SDM will create an Infrastructure RFC in Service Desk and link it to the incident.

Resolving Problems among Team Members. If an identified problem threatens the program quality or cost, we will address the subcontractor directly responsible for the area of nonperformance. In situations where overall contract performance is at risk, HPES will issue the subcontractor a written notice specifying the areas of nonperformance.

Subcontractors and the HPES management team will meet regularly to discuss overall contract performance. These meetings will serve as important forums to identify and resolve potential problems.

Open and extensive communication among team members will foster a cooperative atmosphere in which we can jointly resolve problems at an early stage.

Proactive Communications. Our SDM will maintain transparency with the County through regular communication, reporting on problem progress, and facilitating meetings. The SDM will be accountable for maintaining the relationships, monitoring subcontractor performance, identifying training needs, and escalating issues that require higher levels of attention.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES Service Manager

- Qualifications and Experience – Background and experience in comparable environments

Gartner has stated: HPES' capabilities in event, incident, and problem management for voice communications, visual communications, data equipment, and WAN and remote access solutions are strong and are a reason HPES is an attractive partner for other vendors.

HPES has demonstrated these capabilities to the County for more than 10 years. Moreover, we enjoy corporate reachback when additional expertise or experience is warranted.

Examples of HPES experience in comparable environments include:

- Navy Marine Corps Intranet (NMCI) Continuity of Services Contract (CoSC)
- U.S. General Services Administration (GSA) - Integrated Acquisition Environment (IAE) Federal Service Desk (FSD)
- USA Contact Vehicle IDIQ – DHS USCIS National Customer Service Center (NCSC).

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None

Answers to Specific Questions – Problem Management

2.5.9.1. Describe your proposed approach to staff, address, and remediate systemic and/or recurring problems.

HPES will assign an SDM—and an enterprise problem manager—to be responsible for addressing and remediating systemic/chronic or recurring problems. If necessary, this will be preceded by an in-depth analysis of an issue such as trends associated with tracking Service Desk tickets. Actions can include utilizing Cascade to isolate an issue, or creation of a pan-framework tiger team to address chronic or recurring problems. As part of the lessons learned process, once a trend is identified, action can be taken to correct or improve the outcome.

2.5.9.2. Describe your proposed approach for trend analytics to identify and correct recurring problems.

The HPES enterprise problem manager will be responsible for analyzing quality and reporting trends. This analysis will provide recommendations of appropriate actions to mitigate any negative findings and to propose improvements to drive improved effectiveness and efficiency. As part of the analysis, once a trend is identified, action will be taken to correct, improve the outcome, or prevent future problems from occurring. Our proactive method includes performance-based management and periodic assessments of HPES' KPIs within the problem management framework. Our efforts will include capturing underperforming mission-critical KPI and SLA metrics, escalating them as necessary, and displaying them on the Enterprise Project Management Office (EPMO) status dashboard. We will use this data to identify and substantiate trends relating to similar problems or contributing to problem recurrence, and

develop solutions to address chronic issues. An integral component of our continuous improvement process, we continually assess these indicators to identify negative trends. We will continue to conduct root-cause analysis where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends; thereby ensuring year-to-year continuous improvement.

2.5.9.3. Describe your proposed approach for root cause analyses (RCAs) to remediate identified Incidents and Problems.

HPES will leverage our experience performing Incident management activities in support of problem management, change management, and release management to perform Problem Management activities necessary to identify and resolve the underlying root causes of problems. We will use problem-oriented RCAs to determine underlying causes, identify appropriate resolutions, document findings, and provide recommendations to prevent recurrence of the problems.

Collaborating extensively with County representatives and operating under the guidance of the SDM, our RCA team uses the Six Sigma Define, Measure, Analyze, Improve, Control (DMAIC) methodology; a proven Six Sigma tool. Moreover, we worked closely with the County to develop and hone our 5 Whys approach to identify and get to the root of problems and determine the relationship between different root causes. During the past 5 years, this County collaborative practice has resulted in timely problem resolution and root-cause determination.

5 Whys and the Fishbone Process

The 5 Whys can be used individually or as a part of the fishbone (also known as the cause and effect or Ishikawa) diagram. The fishbone diagram helps HPES explore all potential or real causes that result in a single defect or failure. Once all inputs are established on the fishbone, we can use the 5 Whys technique to drill down to the root causes.

Steps to Complete the 5 Whys

- Write down the specific problem. Writing the issue helps you formalize the problem and describe it completely. It also helps a team focus on the same problem.
- Ask why the problem happens and write the answer down below the problem.
- If the answer you just provided doesn't identify the root cause of the problem that you wrote down in Step 1, ask why again and write that answer down.
- Loop back to Step 3 until the team is in agreement that the problem's root cause is identified. Again, this may take fewer or more times than five Whys.

Finally, in addition to our in-depth knowledge and experience with incident and problem management, HPES is intimately familiar with County needs and long-term vision. We proactively engage at all levels to ensure the IT services we provide and sustain are optimal to meet the County's current and evolving needs. Our leaders will continue working closely with the County to provide and respond to the "over the horizon" view, which includes at a minimum, vigilantly monitoring incidents, problems, and trends as they occur.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.10 Change Management Services (Sched 4.3, Section 2.13)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The change management process itself is the sequence of steps or activities required to implement County-approved changes into the environment and verify the outcomes are as intended. ITIL methodology is the foundation that we employ today on the County account for change management. Overall, HPES is an advocate and champion of successful change management as an integral component of our cross-functional management processes and best practices. In addition to having expertise and direct experience in this critical success area, HPES employs leading technology to maximize its effectiveness and efficiency.

HPES and the County share a belief that, without documented changes, we have no ability to understand the impact on our environment. This is the reason that for years we have worked together to make certain that not only are we documenting and understand these changes, but that we improve and adjust the processes as required. While change management is an important function to facilitate stability of an environment, we also know and agree that we need to be nimble to meet County needs. We bring extensive experience in this critical area, having processed a total of 4,129 potential Requests for Change (RFC), 91% of which were successfully implemented and accepted.

Solution: As mentioned above, the foundation of HPES' change management approach is our proven ITIL certified processes, of which change management is an integral component. A key element of the approach is assigning a single service delivery manager (SDM) per business group to act as a point person and to monitor changes that may impact that space. This service was in place in the past and has proven to be effective, as it provides a single point of contact for the customer.

Rationale: HPES has a well-documented and robust change process in place that we have collaborated with the County to improve. We plan to continue with this process, improving it as needed basis or as the County's business evolves. Our SDMs are responsible for understanding the changes and how they impact their respective business group. SDMs are responsible for making sure that proper communication and discussions for that framework take place and that resources are available to support the RFC owner for testing/validation.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

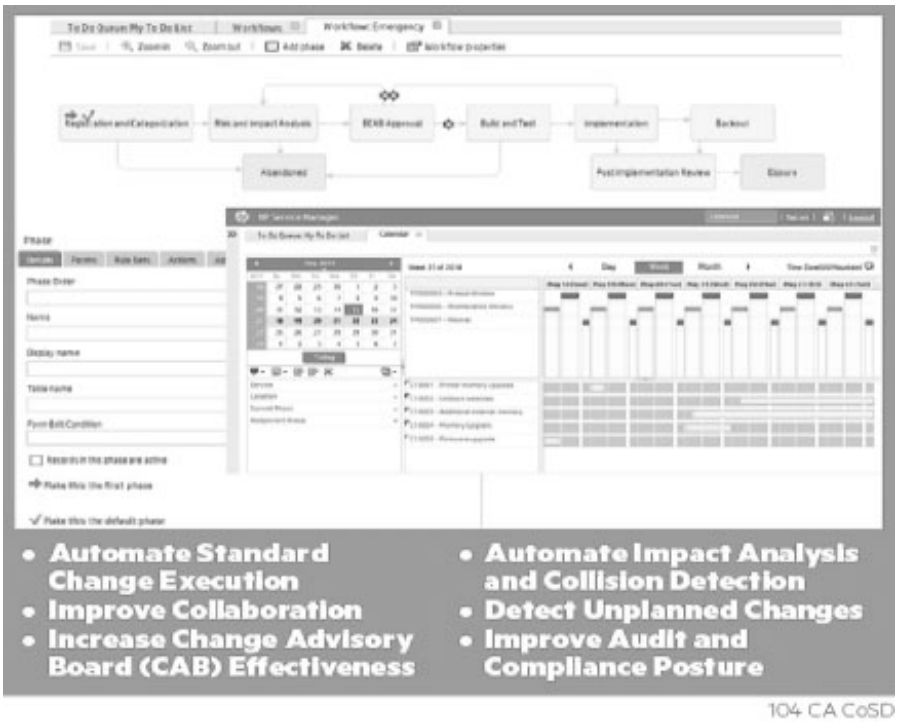
Operating out of our Rancho Bernardo facility, the HPES Change Manager will implement and sustain repeatable, methodically driven change management processes and best practices. Timely, accurate, available stakeholder documentation is an integral part of the change manager's activities, which we will be coordinate with County counterparts as we do today.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The HPES IT Change Management Suite and Services supports multiple types of change requests and mitigates the risks associated with potential requests. Most importantly, it integrates change processes into the broader ecosystem in a cost-effective way, providing full and open transparency and progress reporting. Our new Change Management Suite tool will assist in the continuous improvement needed in this framework, will greatly enhance configuration visibility and stability, as well as monitoring the type and frequency of upgrades that may be required. While costs continue to be constrained with this HPES solution, real benefit will be realized through increased stability and predictability.

HPES IT Change Management is part of an integrated set of ITSM process modules for Service Manager. Figure 20 shows a screenshot of that module.

Figure 20. Service Manager Change Management Module



Change management is fully integrated into Service Manager to fully track and document all changes.

The HPES IT Change Management Suite comes with embedded, out-of-the-box IT Infrastructure Library (ITIL)-based best practices. It creates mechanisms for measuring change process workflows, automates impact analysis, and enhances Change Request Control Board (CRCB) virtualization. We have used the HPE IT Change Management Suite to successfully implement numerous County change requests. The suite also improves collaboration and efficiency across various roles such as change coordinator approvers and managers. Additional efficiencies include reduction in total time needed to process changes, a benefit provided by enabling the changing of approvers via smart phone. This feature facilitates approval of changes anytime, anywhere.

HPES and our partners provide complementary and flexible services—from quick-start packages, to process consulting and design, and more complete implementation packages. Solutions can be deployed onsite, delivered as Software as a Service (SaaS), or outsourced.

The HPES IT Change Management Suite enables the County to create standardized and repeatable workflows. The suite includes built-in best practices with associated industry-standard workflows, forms, and documentation. The suite creates, modifies, and reuses change processes, enabling continuous service improvements. With the HPES IT Change Management Suite, different change types follow different paths. Pre-approved changes for standard requests are expedited while others follow a normal/conventional completion process. Scriptable and repeatable processes, including release management, provide the foundation for reducing risk and enhancing the benefits associated with change.

To help County visualize the end-to-end process, the HPES IT Change Management solution provides a graphical workflow interface. The County can design, modify, and visually monitor multi-level processes. The solution exposes every element of a change process—people, assets, timeframes, tasks, phases, and notifications—in clear, visual terms. This visibility turns the complexity of tracking changes, approvals, task assignments, and planning into easily understandable processes.

Through the HPES IT Change Management Suite, the County is able to coordinate change activities across users and CRCB members, decision-makers, and other stakeholders involved with the change process. The County can also improve planning and collaboration by enabling the suite to send automatic notifications to parties regarding potential changes affecting their respective systems.

The County is additionally able to assign, execute, and track CRCB action items, discussion threads, impact assessments, and voting. The HPES IT Change Management Suite also increases productivity by automating potential collision detection, impact analysis, and risk assessments of change to the business. Moreover, the County can virtualize CRCB functions to enable decisions outside of actual meetings, increasing meeting effectiveness.

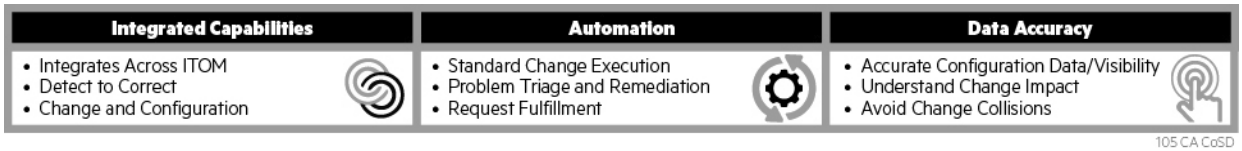
A notable Suite feature is its global forward schedule of change that brings change requests together into a unified common view, providing improved visibility and planning. Change calendars are based on multiple views—including an Outlook-style calendar with timelines by month/week/day/hour, by application, and by implementer. This feature provides insight into the impacts, collisions, and comments of every change request. In addition, the HPES IT Change Management Suite assigns and tracks change windows, freeze periods, and business events, giving the County better control over when changes are implemented.

HPES Service Manager solution and the HPES IT Change Management Suite share configuration and dependency information found in an ITIL-aligned configuration management system (CMS) built on the HPES Universal Configuration Management Database (uCMDB). The Suite automatically and continually performs impact analysis, risk assessment, and collision detection on all change requests. Impacts and collisions are based on infrastructure and application relationships, but they can also reflect timing conflicts in personnel schedules (for example, the people responsible for implementing changes).

The Suite flags all impacted configuration items, potential applications, and associated business services using dependency mapping information. It also compares new change requests to all other pending requests within the same timeframe, and identifies potential collisions that could result in downtime and rework. The Suite calculates a score based on multiple criteria—including historical outcomes of similar changes—for more accurate risk assessment.

As part of the overall HPES Service Manager solution, the HPES IT Change Management Suite is tightly integrated with other ITSM processes and modules—from the logging of change requests through implementation, evaluation, and closure. This includes integration with catalog, request, incident, problem, configuration, and service-level management components of HPES Service Manager. HPES Service Manager delivers connected intelligence. Highlights of this capability are illustrated in Figure 21.

Figure 21. HPES Change Management Service Manager Connected Intelligence



HPES Service Manager delivers transparent Change Management intelligence.

Change requests can automatically originate as incidents or problem outcomes arise. Also employee self-service catalog requests are increasingly the basis for change requests. The companion Service Manager Service Catalog and Request Management modules provide integrated front ends into the change process.

HPES Service Manager Dashboards and reports help IT managers demonstrate value to business stakeholders and provide status information to individual users. Easily customizable dashboards provide

managers and County leaders with quick and concise views into the overall status of the change process while enabling drill-down access to more detailed information.

Automating the complete change process—from assembling requests through implementation and execution of change—speeds the delivery time for standard change requests. Automating change initiation, implementation, and closure tasks also reduces operational costs while improving the quality of service. Integration with HPES Operations Orchestration enables faster RFC creation, change execution and provisioning, and closed-loop validation, reducing the time and staff resources required to manage and implement the overall change process.

Validation and unplanned change detection help close the loop in change management. The HPES Service Manager knows the "managed" state of configuration items (CIs)—or the state in which a CI is expected to be. The HPES Universal CMDB with discovery and dependency mapping information maintains the "actual" states. After a change has been implemented, the managed and actual states are compared to validate that a change was successfully completed. In a similar manner, when a configuration item changes, the HPES IT Change Management Suite compares this actual state of a CI against the record of change requests. Any change that does not have a corresponding change record is identified and will be addressed appropriately—by methods such as creating an incident or a new RFC.

The HPES IT Change Management Suite enables HPES and the County to establish effective IT process controls for change and configuration management. The built-in best practices based on ITIL align with common auditing frameworks such as Control Objectives for Information and related Technology (COBIT). The logging, dashboards, and reporting capabilities help to illustrate the effectiveness of the change controls while also accelerating the production of audit evidence. Standardizing on a common change management process, automating impact analysis and collision detection, validating changes, and detecting unplanned changes all combine to mitigate IT risk.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES' Service Manager.

- Qualifications and Experience – Background and experience in comparable environments

HPES is eminently qualified to provide IM support to the County. Examples of our qualifications and experience include providing the following services to NGEN, HUD, and City of Anaheim:

- Bring more than 300 ISO/IEC 20000 certifications and more than 20,000 IT Infrastructure Library (ITIL) certifications
- Employ more than 1,100 IT Service Management (ITSM) delivery professionals worldwide, managing service quality for our clients
- Manage more than 56,000 changes and change requests per month
- Log and manage approximately 4.4M calls, incidents, changes, and requests each month
- ITSM platform, Standard Reference Architecture (SRA), deployed for more than 500 clients worldwide

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.10.1. Describe your proposed approach for County involvement in the Change Management process.

All changes will receive County approval through a formal change approval process as follows:

- When a change is desired the change initiator will complete an RFC ticket.

- The RFC is reviewed in the internal Technical Approval Board (TAB) review before it is released to County stakeholders.
- The RFC is submitted to the CRCB, which consists of both HPES subject matter experts (SMEs) and County CTO representatives.
- The CRCB reviews the RFC and approves or disapproves the change.
- If the change is approved, the change initiator is notified as well as County end-users, and a Change Release is initiated.
- The Change Release is monitored through implementation and closure.
- A Post Implementation Review (PIR) is completed for each change at the completion of the RFC.

2.5.10.2. Describe your proposed approach for determining and implementing metrics to measure the effectiveness of changes and conduct continuous improvement of the change management process.

The SDM reviews completed changes and can ask for more information about a change in CHG 6.2 (*Request Information*). If this is not necessary, the SDM will determine whether it is necessary for the CRCB to review the change. If so, they will proceed with CHG 6.3 (*Distribute to CRB*). If CRCB review is not necessary, the process ends for that particular change.

The methods and processes used are those developed by the HPES change management team in conjunction with County stakeholders. Our method includes performance-based management and periodic assessments of HPES key performance indicators (KPIs). As an integral component of our quality assurance management program, we continually assess these indicators to identify negative trend lines. We conduct root-cause analysis where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, thereby facilitating year-to-year continuous improvement.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

Release Management Services (Sched 4.3, Section 2.14)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Release management is an engineering process intended to oversee the development, testing, deployment, and support of new releases. HPES is performing release management for the County today. The practice of release management combines the general business emphasis of traditional project management with a detailed technical knowledge of the system development lifecycle (SDLC) and ITIL practices. HPES operates release management services in accordance with these practices, in complete transparency and collaboration with County stakeholders. Our familiarity with these practices and direct County experience with release management requirements informs our method/solution and accompanying rationale.

Solution: The foundation of HPES' Release Management Services is our proven ITIL certified processes, of which release management is an integral component. While the enterprise release manager on the account is responsible for tracking and logging all releases, the SDM for each business group will perform this critical role. The SDM will be responsible for understanding, monitoring, and assisting in the communication of these releases as they are completed in their respective business group.

In addition to the release review meeting that the release manager will hold with the HPES and County stakeholders, releases will be reported in regularly scheduled meetings that the SDM will be required to attend that fall within the scope of their duties. The goal for each SDM is to understand all information related to releases affecting their respective business group, bringing in SMEs if additional information is required.

Release management falls under the governance of the CRCB, which consists of both HPES SMEs and County CTO representatives. All configuration items distributed into production use a formal release management process. HPES develops a Release Plan that outlines the release schedule, content of the release, and backout plans. Release management works with configuration management to make certain that the Definitive Software Library master IT configuration items remain current.

Rationale: HPES has a well-documented release management process in place today. Our hands-on experience with the County informs our proven release management service solution and validates its continued usage. The enterprise release manager will be responsible for continuous improvement and will work in collaboration with the County, as we do today, to facilitate the continued effectiveness of the process. Our SDMs are responsible for understanding the releases and how they impact their respective business group. HPES release managers are responsible for providing adherence to SDLC, ITIL, and HPES best practices. They verify the completed release process is thoroughly documented and communicated to County stakeholders.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The enterprise release manager works out of HPES' Rancho Bernardo.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The goal of release and deployment management is to build, test, and deploy releases into production; to hand over to service operation; and to establish effective use of the service to deliver value to the customer. Effective release management is a bi-product of effective configuration. The accuracy and diligence that HPES will provide in software configuration management (SCM) will be realized by relatively issue-free releases, as they move into production and provide a stable, sustainable, and predictable release.

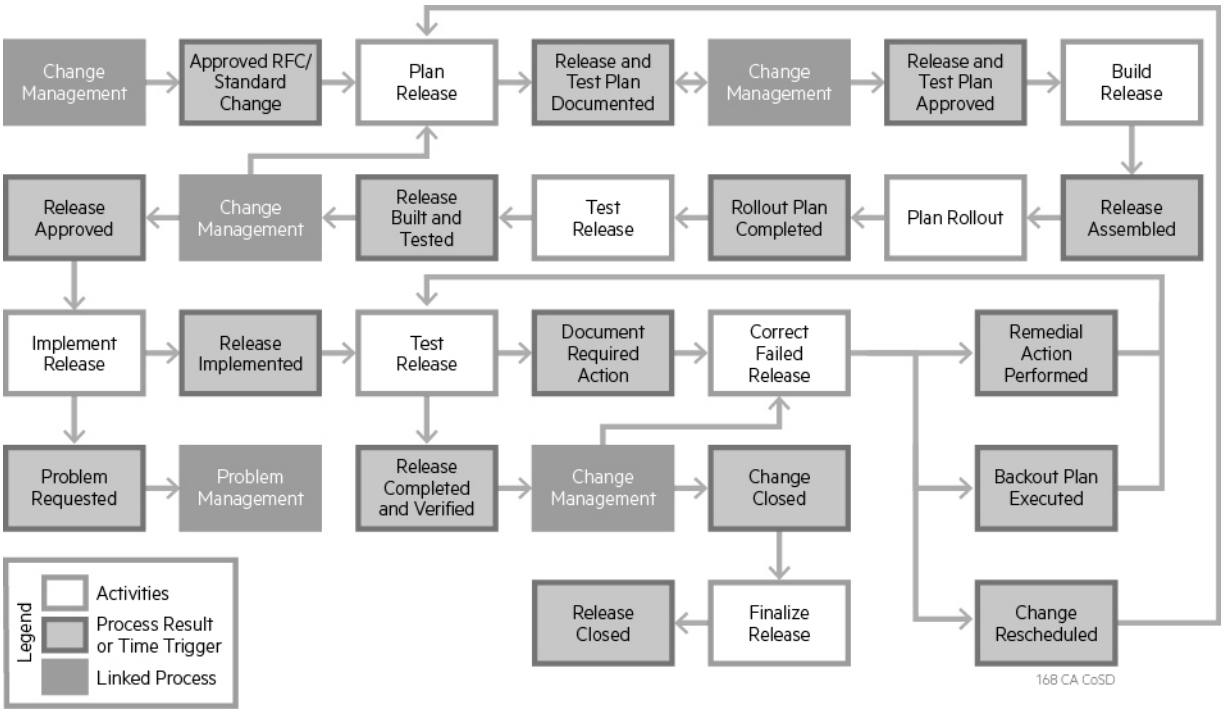
Release management is the process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. Its primary objective is to protect the integrity of the live environment and to make sure that the correct components are released.

Deployment is the activity responsible for movement of new or changed hardware, software, documentation, and processes to the live environment. The term "rollout" is most often used to refer to complex or phased deployments or deployments to multiple locations. Specific objectives of the process are as follows:

- Aligning, coordinating, and communicating release and deployment plans with County projects.
- Successfully building, installing, testing, and deploying a release package to the target environment along with the necessary documentation and training.
- Making certain that the new or changed service and underlying infrastructure are delivered to the agreed service level, providing the service utility, warranty, and level.
- Keeping to a minimum the impact on production services, operations, and support staff and business in general.

Figure 22 illustrates the HPES standard release process.

Figure 22. HPES Release Management Process



Proven process makes sure changes are effectively communicated, properly tested, and configuration controlled.

HPES will bring our change management process and will align with and embrace the County's release management policy.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES Service Manager

- Qualifications and Experience – Background and experience in comparable environments

HPES is eminently qualified to provide IM support to the County. Examples of our qualifications and experience include providing the following services to NGEN, HUD, and City of Anaheim:

- Bring more than 300 ISO/IEC 20000 certifications as well as more than 20,000 ITIL certifications
- Employ more than 1,100 IT Service Management (ITSM) delivery professionals worldwide, managing service quality to our clients
- Manage more than 56,000 changes and change requests each month
- Log and manage approximately 4.4M calls, incidents, changes, and requests monthly
- ITSM platform, Standard Reference Architecture (SRA), is deployed for more than 500 clients worldwide

In addition to our in-depth knowledge and experience with change and release management, HPES has in-depth familiarity with County needs and long-term vision. We proactively engage at all levels to make sure that the IT services we provide and sustain are optimal to meet the County's current and evolving needs. Our leaders will continue working closely with the County to provide and respond to the "over-the-horizon" view, which includes at a minimum carefully reviewing and processing RFCs and subsequent successful implementations/releases.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time

2.5.11 Configuration Management Services (Sched 4.3, Section 2.15)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the

Configuration Management (CM) is the detailed recording and updating of information that describes an organization's hardware and software. For the County of San Diego, we have multiple solutions that feed into one another to provide the information required for the Configuration Management Services. The tools in use today are as follows:

- Apps Manager – Application related information
- Enterprise Server List (ESL) – data center hardware information (severs/storage/network/etc.)
- Asset Manager – Desktop-related asset information
- Endevor – Mainframe
- Serena – Archived source code related to applications
- Team Foundation Server (TFS) –Current source code solution
- AT&T data

HPES and the County understand the criticality of efficiently managed and current configuration information to San Diego County. We collaborate on a regular basis to update this information to verify its accuracy and have worked through a series of improvements in this space. We adhere to the current HPES-provided Configuration Management Plan, which supports/requires close customer collaboration and governs our activities related to CM. We will continue to bring this expertise, experience, and mission involvement to the County and its IT user base, supporting continuous improvement.

Solution: HPES will provide a Configuration Management System (CMS) and multiple CMDBs, accessible through the Service Portal that supports activities associated with recording, tracking, updating, and disseminating the County's configurations for all assets, including network assets. The CMS—integrated across the organization and service frameworks—will support all logical configurations of hardware and software for the services. The CMS contains mappings to physical configuration, inventory data of hardware and software; we will use it to analyze trends as well as manage and reduce incidents and problems. The Service Portal will display all information related to all assets from each tool mentioned above.

HPES will continue to provide software configuration management (SCM) via Apps Manager for the County of San Diego portfolio applications. We will make available the version control history as well as current versions of portfolio code and artifacts, including application code, software tools, and artifacts. Application SCM is part of the program CM and conforms to those policies and procedures.

Discrete item identifiers will be associated with all configuration items (CIs). Applications' CIs include source code, compiled and/or linked code, packaged code, development environment tools, and any related documentation such as user manuals, test scripts, test results, project management documentation, architectural drawings, run books, and helpdesk scripts. HPES SCM will provide physical and logical online libraries for the CM of all software CIs. We will provide hardware-related information from ESL, which is where data center related equipment is tracked and controlled, and Asset Manager, which

includes desktop-related hardware items. HPES SCM is integrated with hardware configuration management data via a feed from ESL to Apps Manager.

HPES SCM will provide three libraries for applications code: two based on platform and one for vendor-delivered media. While Mainframe code will reside in the legacy Endevor library on the mainframe, Windows and midrange code will reside in TFS. More than a version control system, TFS uses a SQL Server database as a means of scaling to large environments and infrastructures. TFS is key component in the life cycle platform, which will enable third parties, customers, and solution providers to extend the base functionality with new features and customize the tool for unique County requirements and initiatives.

HPES SCM will manage third-party vendor code to include contracted code, public domain, purchased, and commercial off-the-shelf (COTS) packages. Third-party vendors will use TFS for development of all applications CIs, unless a program-approved provision is in place for offsite development for that application. Third-party vendors will make certain all code and artifacts are delivered in accordance with the contract. HPES SCM will review the third-party SCM practices and place the vendor deliverables under configuration management for the program.

HPES and County-contracted third-party vendor code developed or maintained offsite will follow County security and HPES SCM standards. The County will be responsible for notifying their contracted third-party vendors of the requirement to follow security and SCM code control. Purchased, public domain, and COTS software packages will be implemented following County security requirements.

Rationale: HPES has well-documented and robust CM tools and services in place, and a foundation on which to build. Our *hands-on* experience with the County informs our proven CM solution, including familiarity with multi-factional integrated CMDBs, and validates its continued use. Our cross-functional configuration managers will be responsible for understanding the interrelated and complementary CM requirements and best practices, and how they impact different frameworks and the greater IT organization. Cross-functional configuration managers will be additionally responsible for making sure that proper communication and discussions for framework take place and that resources are available to manage and support all CM activities including reporting and portal accessibility by County stakeholders.

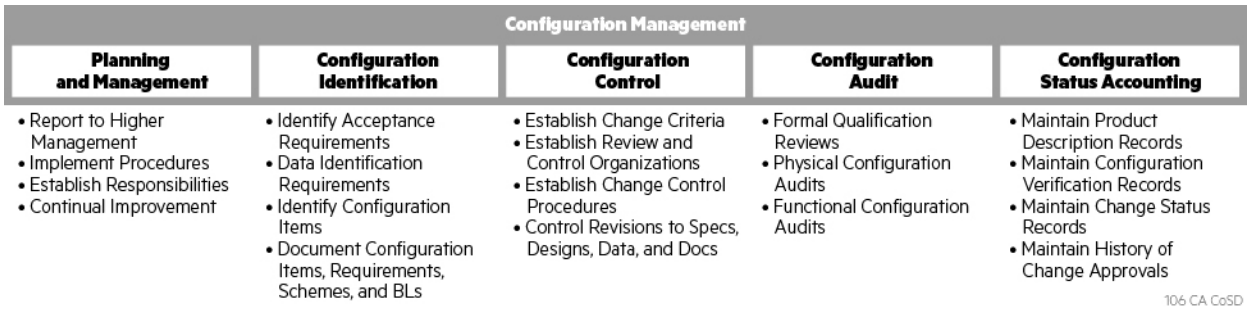
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

CM personnel will operate out of the HPES facility in Rancho Bernardo. AT&T out of their facility on Trade Street.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES understands that CM provides a logical model of services and infrastructure components for planning, identifying, controlling, auditing, maintaining, and verifying versions of CIs in existence within the diverse collection of County assets and software environments. CM is a cross-functional process; it supports other Service Management processes and helps an organization make timely and accurate decisions—Figure 23 illustrates this concept. CM spans all system/software environments, including development, development quality assurance (QA), test, prototype, and production environments. CM provides accurate feature and software inventories as well as tight integration from concept to deployment to production support across disparate service frameworks. Our personnel supporting the County have extensive hands-on experience with version and revision control software, including PVCS, Concurrent Version System (CVS), Subversion (SVN), Team Foundation Server (TFS), Visual Source Safe (VSS), and Git. This experience provides insight into industry best practices and technologies optimal for use by the County.

Figure 23. Configuration Management—a Cross-Functional ITIL Process Supporting Service Management



We deliver IT service quality through proven CM tools and globally accepted best practices

Central to IT Service Management is a CMS and a set of core Service Management tools and databases that provide data to other ITIL or IT Service Management processes to deliver and support IT services throughout the County. The CMS comprises one or more CMDBs that collect and consolidate data from multiple sources into an aggregated view critical for timely and accurate decision-making.

TFS, for example, is a commercial software product specifically designed for CM administration that has been deployed at the County. All types of events that result in software or environment configuration changes are documented and tracked from initiation to closure.

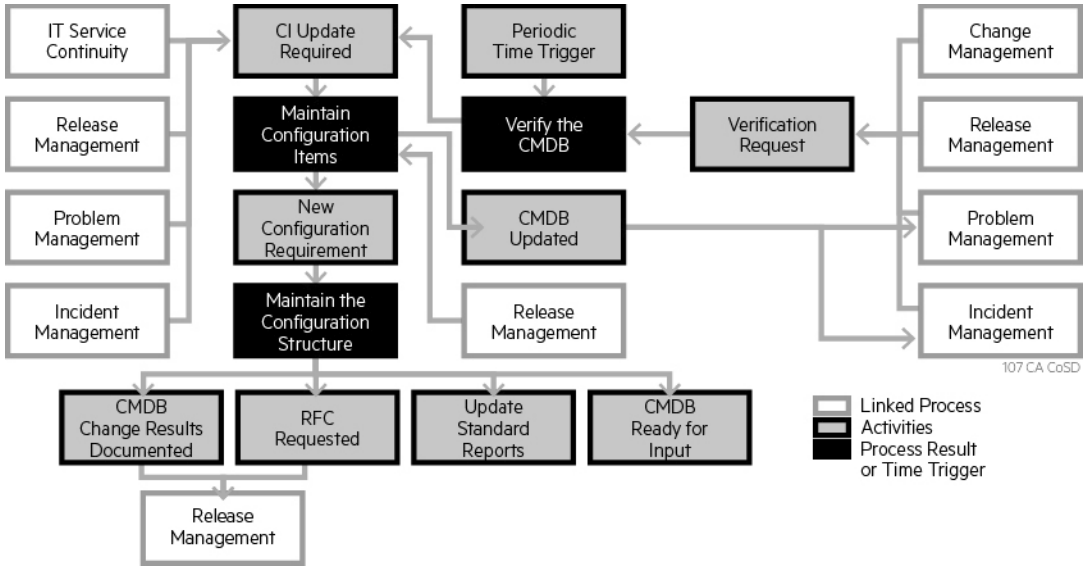
The primary purpose of CM at the County is to make certain that product attributes and technical baselines of all software and systems in use by the County—collectively known as configuration items (CIs)—conform to the documented design for each released software version. This includes the means to document, track, and audit all design decisions and design modifications as well as software and environment build processes that verify the as-built software and host environments exactly match the intended design. CM is an activity that spans many groups across the organization, including management, requirements, process controls, tracking data, development, software tools, archival records, audits, and testing.

County CM includes two primary teams that handle the bulk of the day-to-day CM tasks. The first is a CM process team, led by the County Configuration Manager; HPES currently performs this function and is primarily responsible for verifying that development proceeds according to the organization's documented CM rules. This group, with responsibility for the customized controls and rules, both documents and implements CM processes in a manner that is visible to all personnel; this group also makes certain that released versions of County software products match the required and scoped content planned for that release. This group handles most CM status accounting functions and audit report functions, which are heavily automated through TFS. The organizational investment in TFS as a CM process management system is considerable and has been largely effective. The second group is a development support team, whose duties include maintaining a fully versioned source code repository for each of the major County systems; developing automated build processes; building automatic installation packages; and providing software deployment across development, test, and production environments.

All modifications to this plan must obtain signoff by the County before going into effect. Additionally, quarterly quality reviews will be conducted on the enterprise CM process, and results will be reported to the County. Process user feedback and technology enhancement will be used to continually improve the process.

The primary purpose of CM is to provide a logical model of the infrastructure of a service by identifying, controlling, maintaining, and verifying the versions of CIs in existence in the production IT environment. Figure 24 depicts our standard CM process.

Figure 24. HPES' Standard Configuration Management Process



Delivering quality ITIL-based CM processes that the accuracy, currency and visibility of CIs

To provide accurate and up-to-date information to the organization, CIs need to be effectively managed through the service life cycle; thus data stored within the CMDB must be authorized and controlled by an appropriate authorizing process such as CM, Release Management or Request Fulfillment.

- Automated Tools – Automated systems and tools involved in proposed solution

Automated tools that HPES will use for CM include the following:

- Team Foundation Server (TFS)
- HPES Enterprise Service Management Suite
- Apps Manager
- ESL
- Asset Manager

- Qualifications and Experience – Background and experience in comparable environments

HPES is eminently qualified to provide IM support to the County. Examples of our qualifications and experience include providing the following services to NGEN, HUD, and City of Anaheim:

- Providing CM services to the County since 2006
- More than 300 ISO/IEC 20000 certifications and more than 20,000 IT Infrastructure Library (ITIL) certifications
- Employ more than 1,100 IT Service Management (ITSM) delivery professionals worldwide, managing service quality to our clients
- Manage more than 56,000 changes and change requests per month
- Log and manage approximately 4.4M calls, incidents, changes, and requests monthly
- ITSM platform, Standard Reference Architecture (SRA), is deployed for more than 500 clients worldwide

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.11.1. Describe your proposed solution for the integrated configuration management database that will cover all Service Frameworks.

HPES' integrated CMDB records various CIs along with their attributes and relationships on behalf of the cross-functional service frameworks. Comprised of various framework CMDBs, the integrated CMDB and View will be organized by framework and other key attributes. This will enable individual CMDB CM administration as well as composite or service-wide CM. The HPES configuration manager will be responsible for the integrated databases.

2.5.11.2. Describe your proposed processes to maintain currency and accuracy of the integrated CMDB.

Just as we do for the County today, HPES will deploy auto-discovery tools to maintain accurate and current CMDB CI information.

In addition to our in-depth knowledge and experience with CM, HPES has deep familiarity with County needs and long-term vision. We proactively engage at all levels to make sure that the IT services we provide and sustain are optimal to meet the County's current and evolving needs. Our leaders will continue to collaborate with the County to provide and respond to the "over-the-horizon" view, which includes at a minimum vigilantly monitoring asset inventories and software upgrades. We will make sure all iterations are captured and stored in our CMDB and that County stakeholders are made aware of any anomalies or issues.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.12 Capacity Planning and Performance Management Services (Sched 4.3, Section 2.16)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Capacity planning and performance management, two interrelated but distinctly different disciplines, are integral to HPES' effective and coordinated cross-functional services management.

- Capacity planning is a means of predicting and forecasting resources needed to meet current and future service objectives.
- Performance management concentrates on monitoring and measuring relevant performance metrics to assess the performance of IT resources.

Solution: Focused primarily on the capacity and technical performance of the hardware and software involved in IT services, HPES' capacity planning and performance analysts will collaborate with appropriate stakeholders in determining the resources required and make sure the performance or availability constraints will not adversely affect County business. Response times and quality of services for end users will be used as input and relevant data points to these decisions and performance assessments.

This section covers the process of capacity planning. The process goal is to make sure that IT capacity exists and is matched to the current and future identified needs of the County. The services in scope minimally include application and infrastructure servers, storage, desktops, and networks.

The primary input to this process is capacity planning information, sometimes called performance monitoring metrics in industry literature, such as UNIX and Windows performance information, or network performance information, from various tools. There are other monitoring tools for Mainframe, AS/400, storage, networks, among others. The secondary input to this process is inventory information, which helps the County and HPES to understand the context of the performance information, and to route it to the appropriate County or HPES people. Examples include tools for the data center server inventory, applications inventory, and the billing list of low orgs and their corresponding County business groups.

The primary output of this process is hardware, software, and configuration updates to servers, storage, desktops, and network so that the capacity goal is met. The process involves the assembly of accurate reports of shortfalls, analysis of those shortfalls, and development of a solution to solve any capacity items that do not meet the goal. We employ a cross framework process for ongoing proactive anomaly detection that involves representatives from all frameworks. The responsible framework may also need to obtain County funding approval. The solution is then implemented using existing data center procedures that may include County change approval. Virtual server implementation requires reconfiguration and can be done quickly, while implementation of physical servers may require the installation of new hardware, software, and/or configuration items. Changes recommended and approved will be processed through the change process for implementation. After implementation, the responsible framework verifies the effectiveness of the solution.

Development of Annual Capacity Management Procedures (ACP) is a key component of the HPES solution. The purpose of ACP is to forecast County IT capacity and performance requirements on an annual basis and reaching forward. The requirements definition, based on historical performance, provides the foundation for continuous improvement while making sure that a cost-benefit-analysis (CBA) confirmed County IT operations and service delivery. The ACP balances needs over the long term to optimize the resource workload expected in coming years. The primary inputs to the ACP process are historical performance information during the past year and the CTO technical roadmap, so that the forecast encompasses all data needed to meet immediate and extended future capacities and all service levels.

The output from this process will be the projections for the next 2 years of IT capacity necessary to support the forecast, including identification of OS upgrades required to support the forecasted capacity.

Because of the strategic significance and planning impact to service delivery for the future of the environment, it is important to understand the basic assumptions underlying the ACP plan including:

- Business forecasts are preferred over historical trends
- ACP output identifies future issues needing solution, and provides many supporting details, but does not produce the solution itself
- Holdovers from the previous year assumed to be addressed in the previous year. That is, current shortcomings are ignored.

The initiation of the ACP for report delivery to the County for review and approval begins during the mid-October timeframe, a sufficient lead time for delivery of this annual report. The ACP report framework components for the County program are discussed in the following sections.

The cross-functional capacity and performance management process assembles the prior year's historical information, including business forecasts, and generates the forecast during the planning period, including identifying OS upgrades if required.

The ACP is used to tune the performance management process for the new workload, and to selectively identify problems/opportunities that should be undertaken as projects to mitigate some of the workload. The performance management process collects current system capacity and/or performance data and

performs predictive analysis to identify when the current capacity will exhaust. This data is stored and used in annual capacity planning as historical information.

New desktop hardware technology is reviewed annually by desktop engineering. Capacity and performance specifications for desktop hardware and desktop applications in use or planned will be reviewed with vendors to accommodate current and future County requirements and expectations. A report of recommendations is presented and reviewed with the CTO. The information collected throughout the year is incorporated into the ACP, providing adequate desktop services to maintain service delivery.

Rationale: HPES has extensive experience in IT services capacity planning and performance management, both globally and locally. Our hands on experience with County IT requirements and challenges confirms our proven methods and best practices and validates their continued use. Our capacity planning and performance analysts will be responsible for understanding the interrelated and complementary requirements, and how they impact different frameworks and the greater IT organization. In addition to discovering and analyzing critical touch points and KPIs, our analysts will thoroughly document and report their findings and activities and make the information available to County end users through the Service Portal.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The positions required to provide capacity planning and performance management services are capacity planning manager and IT capacity planner. These personnel will reside in HPES' Rancho Bernardo facility. Network capacity planning will be augmented by AT&T operating out of their facility on Trade Street.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES capacity management is an ITIL-compliant service that helps prevent business disruptions by proactively managing system use and capacity. Making sure the right capacity is always available can mean increasing capacity based on County business and IT needs, or reducing or reallocating capacity so the County only pays for the necessary hardware, software, and needed support.

We will proactively and continually monitor capacity so that availability does not fall below 75% and potentially result in degraded performance and a net-negative impact to the business. We will also monitor and identify capacity usage, possibly indicating architecture design or program configuration anomalies.

Capacity management makes sure the County IT infrastructure is ready to meet the demands of users at agreed operational levels today and that IT services have the capacity to support future requirements. This is accomplished through collecting, analyzing, and reporting on capacity statistics and assessing the impact of County-planned projects. We will work closely with County to plan and budget IT capacity based on changing business requirements, as well as recommend improvements for optimization of infrastructure investments.

Data collected through automated reporting will be provided with an understanding and analysis of in-scope components' current capacity consumption. A collection of reports will display standard component utilization metrics, such as memory and CPU capacity. The lowest level of detail available will help with capacity planning and management.

We will group, and trend by day, all data for a single calendar month or monthly for the past 12 months.

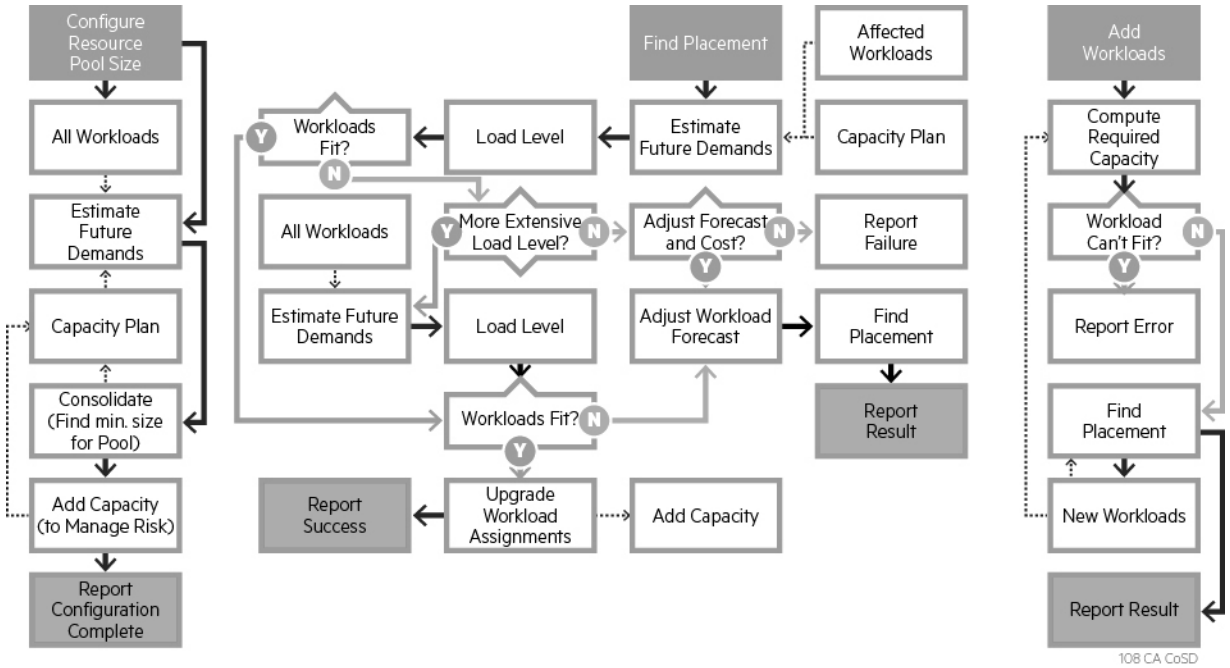
County employees with access to the Service Portal may view the capacity reports at will, giving them the freedom to access data and reports as required. They can export reports to Adobe Acrobat, MS Excel, MS Word, or Rich Text format, enabling further analysis, combining with other data, or including in presentations and other documents.

Using automated scripts, HPES will extract use data monthly from data collection servers and load it into the capacity management application. On a monthly basis, we will produce a forecast report using historical data that is trended over 12 months. Graphs include installed, usable, and forecast capacity data points.

The capacity management process relies on the key concept of a capacity management plan, which is a calendar-based data store that keeps track of workload identities, forecasts, and resource access quality of service requirements; resources that are associated with a pool; and assignments of workloads to resources. As a calendar-based data store, the plan keeps track of such information as a function of date and time and uses it to support capacity planning.

Figure 25 illustrates several aspects of our capacity management processes. "Configure resource pool size" will be used to reduce capacity fragmentation by periodically repacking or consolidating workloads in a pool. "Find placement" balances loads, dividing them evenly across resources. It has two stages—if no resource is able to support the resulting capacity requirements then we will attempt a larger scale rebalancing of workloads, adjust workload quality of service requirements, or combine the two approaches. "Add workload" will report whether a placement can be found for a new workload.

Figure 25. (a) - (c). HPES Examples of Capacity Management Processes: (a) Configure Resource Pool Size, (b) Find Placement, (c) Add Workload.



HPES provides a comprehensive approach to capacity management.

- Automated Tools – Automated systems and tools involved in proposed solution

The automated tool we will use to provide capacity planning is HPES' Global Delivery Capacity and Performance Management (GDCPM) tool. This is data warehouse that includes many database, storage,

telecom, and networks. Other types of infrastructure data include system/server capacity management (forecasting and trending) metrics, availability metrics, and Performance management data.

- Qualifications and Experience – Background and experience in comparable environments

HPES is eminently qualified to provide IM support to the County. Examples of our qualifications and experience include providing the following services to NGEN, HUD, and City of Anaheim:

- over 300 ISO/IEC 20000 certifications
- over 20,000+ ITIL certifications
- over 1,100 IT Service Management (ITSM) delivery professionals worldwide
- managed over 56,000 changes and change requests per month
- Log and manage approximately 4.4 million calls, incidents, changes, and requests monthly
- ITSM platform, Standard Reference Architecture (SRA), is deployed for more than 500 clients worldwide.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.12.1. Describe your proposed approach to monitor, analyze and optimize capacity and performance in a virtualized data center.

Capacity planning and performance optimization in a virtualized environment requires consolidated views across multiple IT silos of the virtual infrastructure, where consumption and waste can be understood in the context of the real-world business processes and applications. To make sure that the County IT infrastructure can support agreed to or target service levels in a cost-effective and timely manner, HPES will provide capacity planning and performance optimizations as follows:

At its simplest level, capacity planning can be thought of as the task of balancing supply (CPU, memory, storage, I/O) with demand (applications/SLAs). The virtual environment, however, introduces new twists to traditional capacity planning practices.

- Virtualization involves a different level of abstraction, where the relationship between shared resources is in a constant state of flux. Although enterprises view the supply side of capacity planning as pools or clusters of virtual resources, they must also understand which cluster or pool to use for an application and the broad impact on a virtual environment. For example, our virtualization specialists will determine which clusters or pools need more resources as well as how updating virtual resources affects other resources. They will make recommendations on how to deal with virtual machine (VM) sprawl (a proliferation problem), and when to reduce VM resources if we believe they may be needed soon, but not currently.
- Although capacity planners have always been concerned about waste (or how much oversupply to have in reserve), the concept takes on new meaning in virtual environments, where the ease with which VMs and applications can be created has led to VM sprawl. Depending on the environment, waste due to VM sprawl can be considerable. Without proper insight into consumption requirements, enterprises risk vastly overestimating the resources needed to support their virtual environment.
- VMs do not exist in isolation; they run complex (often multi-tiered) applications that support many lines of business. Being able to profile how applications and business departments use (or potentially waste) the underlying physical resources is key. Even without a formal chargeback process, organizations need to understand how resources are being consumed so budget considerations can be calculated and sensible use of resources can be encouraged to meet demand.

HPES VM specialists are experienced in VM environments and demand nuances, and will share this experience and expertise with our capacity planning and performance analysts to make sure County virtual environments are accurately planned, used, and measured. We proactively and continuously monitor capacity so that availability in the virtual environment does not fall below 75% and potentially result in degraded performance and a net-negative impact to the business. We also monitor and identify capacity usage, possibly indicating architecture design or program configuration anomalies. Should virtual capacity or performance require additional resources, we will immediately substantiate and initiate appropriate requests and notify appropriate stakeholders.

Once virtual environment considerations are factored in to the demand and use parameters of capacity planning and performance optimization, normal activities will make sure the following occurs:

- HPES capacity management is an ITIL-compliant service that helps prevent business disruptions by proactively managing system use and capacity. Making sure the right capacity is always available can mean increasing capacity based on County business and IT needs, or reducing or reallocating capacity so you pay only for the hardware, software, and support needed.
- Capacity discovery occurs through collecting, analyzing, and reporting on capacity statistics and assessing the impact of the County's planned projects. We will work closely with the County to plan and budget IT capacity based on changing business requirements, as well as recommend improvements for optimization of your infrastructure investments, including people, processes, and tools.
  - We will extend this environment with sufficient capacity to accommodate increased workloads to include a new purpose-built Managed Private Cloud (MPC) environment. The MPC environment is a highly standardized environment with high-redundancy and scalability.
- Utilization reporting uses data collected through automated reporting to provide an ongoing understanding and analysis of in-scope components' current capacity consumption. A collection of reports displays standard component utilization metrics, such as memory and CPU capacity. The lowest level of detail helps with capacity planning and management.
- The capacity trend reporting feature provides more advanced reporting capabilities than the standard use report. Using automated scripts, we will extract use data monthly from data collection servers and load it into the capacity management application. On a monthly basis, we will produce a forecast report using historical data that is trended over 12 months. Graphs will include installed, usable, and forecast capacity data points.

In addition to our in-depth knowledge and experience of capacity and performance management and conventional (on premise) architectures and cloud-based virtual architectures, HPES is intimately familiar with County needs and its long-term vision. As such, we will proactively engage at all levels to make sure our IT services are optimal to meet the County's current and evolving needs. Our leaders will continue working closely with the County to provide and respond to its "over the horizon" view.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

Disaster Recovery Management Services (Sched 4.3, Section 2.17)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES enjoys a rich history of responsible and timely IT disaster preparedness and recovery management. With mission critical IT solutions deployed globally, often in hostile environments, we recognize the importance of proven, reliable disaster recovery (DR). Serving as a recognized authority in this critical area of enterprise IT readiness, HPES enables organizations and municipalities worldwide to:

- Recover disaster - Prompt recovery of services, with minimal disruption and data loss
- Measure and audit the County's ability to meet recovery objectives
- Continually review and improve continuity policies and practices
- Automatically detect infrastructure vulnerabilities that could impact DR readiness or availability
- Validate that production and replication environments are synchronized
- Enterprise Voice and Real Time Communications systems local survivability and cellular back-up.

Solution: Implemented as part of the data center and network frameworks, HPES' DR management services will provide strategy, process, type, methodology, locations, documentation, and prompt restoration of services. Our solution is a subscription model, based on the County's currently-specified Recovery Time and Recovery Point Objectives. Applications with a 72 hour RTO will be recovered from replicated Virtual Tape Library (VTL) backups. Applications with a 48-hour RTO will have their DR servers mounted to replicated SAN storage. Under a subscription model, the server hardware "subscribed" to by the County is leveraged, provisioned with County images and applications on an as-needed basis to support DR tests, or actual disaster events. However, if shorter recovery times are required in the future, we can implement active/active and/or active/passive solution, using dedicated server hardware for web, application, and data layer recovery.

During transition, we will validate ongoing DR policies and procedures including:

- Portfolio application priorities and Recovery Time Objectives/Recovery Point Objectives (RTO/RPO) requirements including:
  - Validation that restoration times meets County requirements
  - The server strategy (subscription using replicated backups or SAN data, or one of the dedicated hardware options above)
  - Data synchronization and replication plans
  - Rationalization of licensing costs.

Our solution is based on F5 Global Traffic Manager (GTM) and Akamai. For active/active, should it be required, we would use a synchronization technology such as SQL server Always-on architecture -or Oracle Data Guard architecture. Our technology Continuity of Operations (COOP) professionals, whose primary mission is to build a robust DR program for the County, will write a viable and executable DR plan and schedule and manage DR exercises. Upon declaration of a DR event, HPES will execute the County Disaster Recovery Plan (to be developed during transition) that includes:

- Recovering and resuming full operations including all supporting infrastructure and networks of:
  - County requirements
  - Priority 1 applications within 48 hours
  - Priority 2 applications within 72 hours
- Recovering all County data repositories with a data loss of no greater than 28 hours.

Rationale: HPES has well-documented and robust disaster recovery tools and management services in place. Our hands-on experience with the County informs our demonstrated DR solution, including familiarity with synchronization requirements, recovery objects, and validates their continued usage. Our remotely located disaster recovery managers will be responsible for understanding the inter-related and mandatory backup and synchronization requirements and best practices, and how they may affect different frameworks and the County. Our enterprise service delivery manager will be the County point person and the conduit for information flow between remote disaster recovery managers and the County. Our enterprise service delivery manager (ESDM) and remote DR managers will be responsible for communication, managing resources, and supporting all DR activities, including during and after the event, which will include a complete report to the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

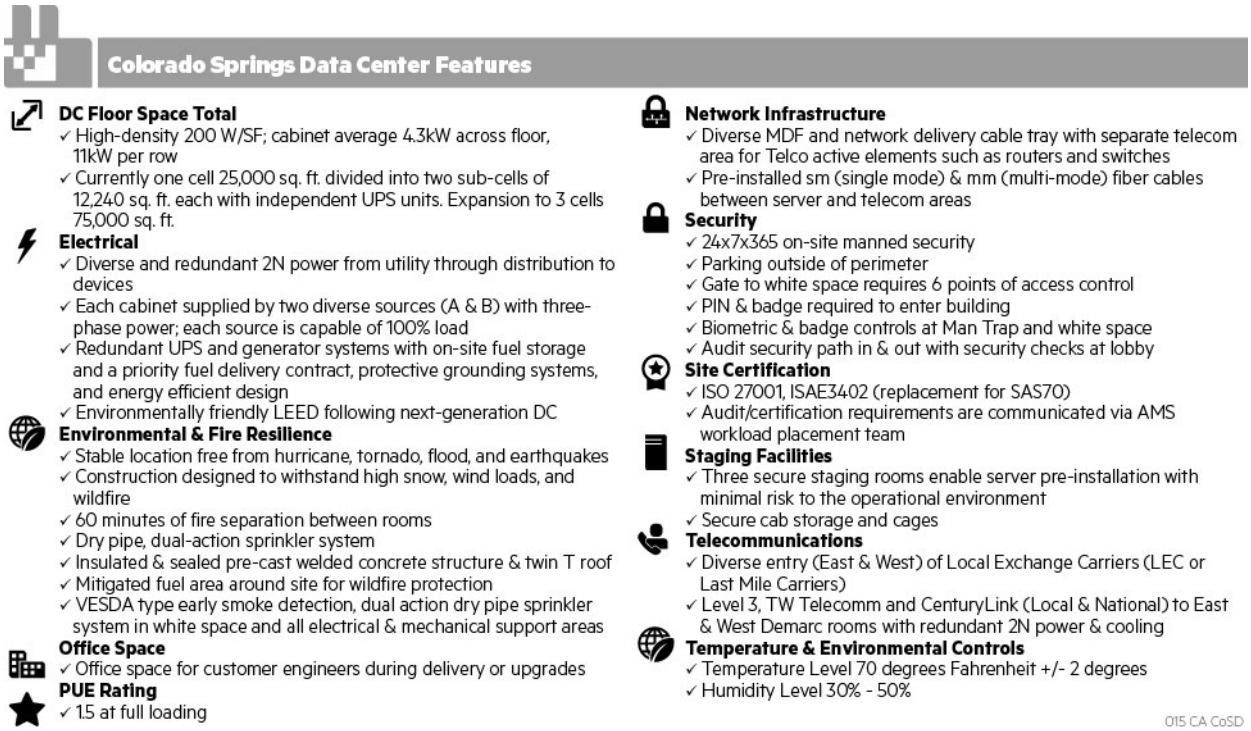
We have selected our Colorado Springs, CO Data Center (CSDC) for the County's recovery site, connected via dedicated 10GB circuit, providing data replication. We will be able to provide a wide variety of disaster recovery services—dedicated to shared and/or hybrid solutions—at this central location.

Our highly experienced continuity professionals will write, maintain, and exercise County DR plans and data center management professionals will maintain the hardware, replication, and synchronization aspects of the solution. Connectivity and synchronization with CSDC will include HPE's Tulsa production/development center and the County operations data center, as well as the AT&T POP, DR POP, Tower 9, Lemon Grove, and future sites as required. Coordination will be managed by the HPES ESDM.

The CSDC is a purpose-built, SSAE16-audited, world class data center designed to meet the demanding needs of the modern computing environment. The Tier III data center design provides a completely redundant and continuously operating facility with infrastructure built with hot-swappable components, redundant power supplies and fans, compact flash, multiboot support, and always-on management. Data synchronization and replication will be determined by each application's RTO and RPO, and VM server versus physical server recovery methodology. Appliances can be deployed in traditional active/standby configuration or horizontal clusters (active/active) to achieve high availability and application-level failover. HPES' CSDC MDRS facilities include locking cages, cabinets, and racks to meet County physical security requirements. This facility is used to provide DR and data backup services for HPES' USPS clients as well as HPES Corporate.

Access to the CSDC is highly restricted. Access to network and HPES computer equipment, storage media, critical support areas, and operations documentation is only granted to authorized personnel. Security consoles linked to alarm systems and closed circuit TV (CCTV) cameras are manned. Security cardkey readers protect all doors leading into the data center, and issuance of cardkeys for physical access to the facilities is controlled through a request and approval process. Figure 26 depicts features and capabilities of the CSDC.

Figure 26. CSDC Features and Capabilities



Providing comprehensive, full-service data center capabilities that facilitate continuous processing and operational stability.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

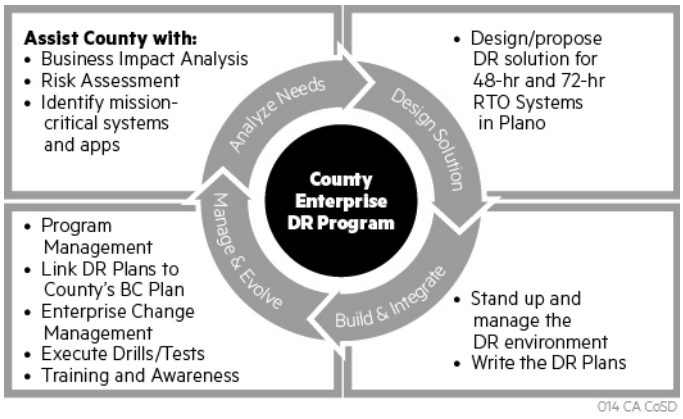
HPES takes a holistic, yet modular, approach to manage the County's enterprise DR program, as depicted in Figure 27 The methodology is comprehensive, derived from decades of experience, and is built on industry best practices and standards of the Disaster Recovery Institute International (DRII) and ITIL. This model defines four phases in the DR life cycle of a business continuity program—Analysis, design, build and integrate, and manage and evolve. The DR program includes periodic and short-notice drills to validate the processes. These are in accordance with the County DR plan and coordinated by the ESDM.

This model is flexible and adaptable, enabling phased implementation for the overall continuity program and for the County to enter and exit the life cycle at any point within the methodology process path.

The design phase is an enhanced DR (EDR) solution and the subscription DR solution for the 48- and 72-hour RTO systems respectively.

HPES' delivery team will start with the build and integrate phase and stand-up the DR environment while our continuity professionals begin the preliminary stages of drafting the DR plan. In this phase we will provision the replication circuit between the Tulsa data center and the CSDC recovery site. We will verify that data replication is occurring accurately and as planned. At the end of the phase, HPES will perform a tabletop exercise of the DR plan to validate its functionality and address any deficiencies found during the exercise.

Figure 27. County Disaster Recovery Program



The County's DR program provides standards- driven DR and enables operational continuity.

At the conclusion of the tabletop exercise, the management and evolution phase of the DR program life cycle will begin. In this phase HPES and County will agree on the master DR exercise calendar and work closely together to reflect the production changes into the DR environment in a methodical and timely manner. It is extremely important to keep the DR plan in lock-step with enterprise change management. HPES will provide required training during this phase to make sure it is operating as expected.

In the analysis phase, HPES will work with County and assist in yearly undertakings such as a Business Impact Analysis (BIA) or identification of critical systems and apps. Table 15 outlines the features and benefits of our approach.

Table 15. Critical System Features

FEATURES	BENEFITS
CSDC Tier III, HPE corporate DR services, Federal DR clients, and is highly redundant and secure	• Highly skilled and experienced engineering, operations, security and program management resources • Experienced testing and compliance personnel
Network design that is redundant and secure, with automated GTM and load balancing capabilities with multi-layered firewall design	• Uses the skills and experience of our network operations personnel • GTM automation works to reroute IP traffic in the event of a declaration • Automatic and transparent recovery and continuity of service
Automated, continuous host-based replication for 48-hour RTO systems	• Automated, real-time maintenance of host images and data integrity • Near real-time RPOs • Can failover or fall back virtual-to-virtual or physical-to-virtual systems
Industry recognized DR PLANNING leader (Forrester-Traditional Disaster Recovery Service Providers)	• Highly skilled, trained, and BCM-certified personnel • Comprehensive development methodology • Experienced with Federal standards including NIST SP 800-34 Rev. 1
Continuous Process Improvement Loop	• Independent monitoring during exercises followed by after-action lessons learned to identify and integrate ways to improve DR processing

The DR plan will be a cohesive document that includes an auditable overview, team structures, responsibilities, contact information, detailed recovery procedures, and recovery site activation aligned with NIST SP 800-34 Rev. 1. Developed using HPES templates, the plans will be stored in a secure SharePoint site with access to authorized personnel only. HPES will design the plans to enable hand-off to County staff to complete their portion of the recovery and for data validation. HPES will also work with the County to create disaster definition and declaration processes relative to this proposal. As input to the DR plan, the County will need to provide complete data on application interdependencies, as well as application to production infrastructure mapping.

After approval, the DR plan will be reviewed during an initial tabletop exercise. This exercise will be conducted with County staff and operational leaders, who will play an active role in the event of a disaster, to fine-tune plan details and serve as a means to provide initial training to the County and HPES. Additional training will be provided to the County and HPES delivery team as needed.

As a standard operating procedure, HPES incorporates client change management processes into the DR life cycle. Any change to the production environment must be captured in the DR plan and the MDRS environment or it becomes impossible to maintain a viable and executable plan. Therefore, our lead continuity professional on the account will be a member of the change control board.

Annual DR Exercises

HPES will schedule, plan, and lead one DR exercise annually in cooperation with the County. HPES and the County will agree on the strategy for the testing scope and a master schedule. Depending on various elements such as impact to the production environment or availability of the resources, exercises may be live or table-top exercises. When possible, a DR exercise will include an entire IT production site, or exercises will be for all the applications in a given recovery tier or for a logical grouping of the applications. HPES will coordinate the following items:

- Laying out the entire exercise process with specific milestones, objectives, and metrics for each scheduled exercise
- Putting measures in place that track objectives
- Coordinating and preparing with the County application teams, users if desired, and any third-party vendors required
- During the exercise, measuring and tracking recovery timelines according to the County's RTOs and RPOs
- Documenting exercise results in a formal report, including comparison of the results to the measures and goals established, action items from the exercise, and recommendations on how the recovery process could be improved to be faster and more reliable
- Updates to plans as needed

- Automated Tools – Automated systems and tools involved in proposed solution

None at this time.

- Qualifications and Experience – Background and experience in comparable environments

HPES has been providing customers with DR and business continuity services since before 1984. As one of the major continuity service providers, our experiences provide the foundation to develop a comprehensive DR plan to support the County with effective preparation, response, and recovery from disaster events. Our team of highly trained, experienced, and certified professionals will provide the expertise necessary to manage the full life cycle of comprehensive DR services necessary to provide continuity of services in the face of a disaster. Our planning, testing, training, and execution are based on methodologies perfected through decades of experience and on industry best practices.

Examples of HPES' experience in comparable environments include:

- Navy Marine Corps Intranet (NMCI)
- Defense Manpower Data Center (DMDC)
- Michigan Department of Natural Resources (MI DNR), Second Generation Retail Sales System (RSS-II)

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.12.2. Disaster Recovery and Business Continuity Specific Questions

None at this time.

2.5.12.3. Describe your requirements for County involvement with the Disaster Recovery plan.

- Define RTO requirements
- Review/approve DR plan
- Participate in drills and tests.

2.5.12.4. Describe your proposed approach for County Data recovery and restoration to meet the Service Levels.

For County data repositories restoration with no greater than a 28-hour data loss, we propose data synchronization and replication that includes the County's immutable storage, live data, and virtual tape libraries.

For the systems and applications with a 48-hour RTO, we propose HPES' EDR. This solution, which consists of replicating data center data asynchronously between the Tulsa production site and the CSDC recovery site, will meet RTOs in as short as 4 hours. Therefore, we are confident it will meet the 48-hour RTO stated in the RFP.

For the systems and applications with a 72-hour RTO, we propose:

- Deploying virtual tape libraries between the production and recovery sites, using the same replication circuit provisioned for EDR above. We subscribe to physical or virtual servers for DR tests or during a true disaster event. HPES continuity professionals will stand up these servers within 12 hours of the disaster declaration, leaving 60 hours of the balance of the RTO to reconstitute the applications and data on the servers. Because virtual tape library (VTL) data is readily available at the recovery site, this solution will meet the stated 72-hour RTO.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.13 Identity and Access Management Services (Sched 4.3, Section 2.18)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES is dedicated to the Identity and Access Management (IDAM) security discipline that enables the right people to access the right resources at the right times for the right business reasons—while preventing unauthorized or intrusion attempts. HPES uses IDAM technology to initiate, capture, record, and manage user identities and their related access permissions. Our globally proven, fully automated

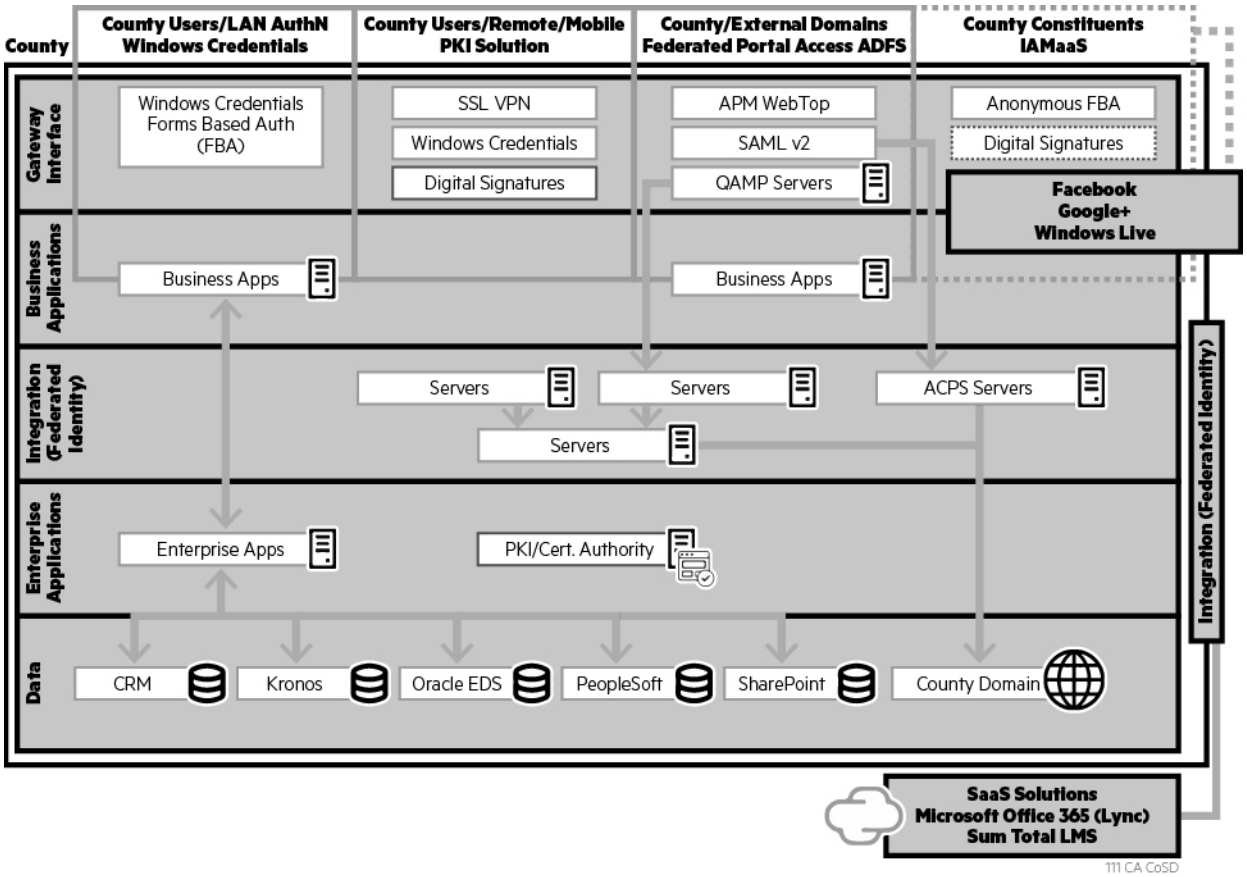
approach makes certain that access privileges are granted according to a singular interpretation of policy and that all individuals and services are properly authenticated, authorized, and audited. Recognizing the critical importance of IDAM, particularly in light of emerging technologies and cloud-based infrastructure migration, HPES' expertise and experience in this area—combined with our familiarity with the County—enable us to offer an industry/enterprise-proven tailored IDAM solution.

Solution: HPES' approach to the County IDAM solution is to continue to evolve and improve the County's existing investments in PeopleSoft, Active Directory (AD), and Oracle IDAM to provide an overall platform to protect and manage individual identities, their authentication, authorization and roles, and privileges. The starting point or foundational element of the solution is the Oracle IDAM platform, which is an industry-leading, end-to-end security solution—providing components that protect applications, data, documents, and cloud-based services through a combination of flexible authentication and single sign-on, identity federation, and risk-based authentication and authorization. The County's IDAM solution—starting with the Oracle platform and extending to the current County Active Directory, PeopleSoft, Public Key Infrastructure (PKI), Active Directory Federation Services (ADFS), and the HPES Identity and Access Management as a Service (IAMaaS)—provides an integrated, modular architecture. This architecture provides the County with the flexibility to deploy a complete solution that will enable the integration of current platforms, existing applications, and third-party security services into a single solution—offered at a single price point. We will implement IAMaaS post-Transition if optionally requested by the County as a Transformation project.

The high-level scope of this solution is to use Oracle Identity Manager as the basis to manage the user accounts across various applications and integrate identities within Active Directory, PeopleSoft, the HPES IAMaaS, and third-party applications that contain County identities. The Oracle Identity Manager will act as a single point of user management for the administrator to create users and authorize the user to access the relevant resources across the County, while allowing the other key platforms that contain identities to continue. The Oracle Access Manager solution will secure the application access with respect to organization applications. Figure 28 shows the main elements of the proposed County Identity Management solution, which makes use of existing capabilities while expanding the solution to meet all of the requested functions for the County. Depicted in Figure 28 are the four main "kinds" of identities that the County must manage/administer. These identities are as follows: "classic" referring to County users that exist on the County network, County users that are remote or "off-premise," and County identities that require a federated relationship with external services such as County partners, residents or visitors.

By implementing the architecture illustrated in Figure 28, each "kind" of County user will be able to be managed in a low-risk, cost-effective, controlled, and secure manner so that management of the identities can be performed from a single point yet extend to each kind of user. Included in this solution is access to the County business applications, federation capabilities, enterprise applications, and County data sets.

Figure 28. San Diego County Functional Architecture



Providing secure IT services through comprehensive IDAM.

Rationale: The rationale for the IDAM solution for the County is to:

- adhere to the County's current IDAM strategy and direction;
- minimize risk and cost to the County by leveraging the County's current investment in Oracle IDAM platforms;
- build on the current Active Directory and Active Directory Federation Services (ADFS)

This approach will minimize expense by leveraging the County's investments in Oracle, PKI, Active Directory, and ADFS; lower the technical and operational risk by expanding on existing platforms; and will enable the County to continue to execute its Identity Management Road Map and Strategic Plan.

The following Oracle elements are currently implemented within the County's 11g Suite – Identity Manager, Access Manager, Internet Directory, and Virtual Directory—integrating them with Active Directory, PeopleSoft, and HPES IAMaaS. Table 16 details each of the main elements of the integrated solution and what specific function they provide.

Table 16. Solution Integration Components

PLATFORM	CURRENT BUSINESS USE CASE	FUTURE BUSINESS USE CASE
Oracle Identity Manager (OIM)	Integration with PeopleSoft	• Onboarding for new employees • Manage Health Care partners for Curam

PLATFORM	CURRENT BUSINESS USE CASE	FUTURE BUSINESS USE CASE
		• Provisioning applications users (Curam, EDPP, EBS, OBI, and other applications) • Manage privileged accounts in AD and UNIX • Cloud-based Identity Management System (IAMaaS) to manage County resident credentials (Transformation project)
Oracle Access Manager (OAM)	• Provides Single Sign On (SSO) to 25 applications to County employees as well as firewall department users • Federation with firewall department organizations as Service Provider	• Continue to integrate more County-owned applications. • Federation with third-party vendors as Identity Provider. Provide this capability through IAMaaS Federation Hub if necessary. • Provide SSO capability to third-party vendor applications like Adobe Cloud, Adobe Analytics, LexisNexis, ABC Legal, Accurint, Attorney's Brief, Empinfo, e-Oscar, Inverify, Past-Employ, The Work Number, Westlaw, and Pacer. • Provide risk-based multi-factor authentication capability for IDAM protected applications. • Provide SSO capability to State-owned applications like CSE (CCSAS), CA Central, CALWIN, ECSS (State IVR), KidStar, and SAT C3.
IDAM architecture	• Provide High Availability within one data center	• Re-architect IDAM to provide Zero Downtime Architecture
IDAM Infrastructure monitoring	• Monitor software components manually	• Leverage licensed Oracle monitoring tool, Oracle Enterprise Manager (OEM), to monitor IDAM infrastructure (both software stacks and data base).

The following list details the progressive steps of the Identity Management solution and details what is being done today and what HPES recommends for the future:

- Current Effort – Oracle Federation Manager is currently deployed with Service Provider active and Identity Provider not active. Based on the existing request from Department of Child Support Services (DCSS), we are planning to implement the Federation Acting as Identity Provider upon approval.
- Future – Develop a process for auto-onboarding new employees based on the information in PeopleSoft to create the AD identities.
- Future – Expand the use of the existing platforms into all County business group and partners as well as work with current San Diego partners with expansion to others.
- Future – Use the HPES IAMaaS solution to expand to County residents and to act as the Identity Manager for County residents.
- Future – Re-architect the solution to become the Zero Downtime solution.
- Future – Federate with County third-party vendor applications.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The HPES team supporting the County will work closely with the County CIO, CTO, and supporting staff and provide a close-knit working environment that will allow for direct communication, service, and for the County to be able to reach out directly to HPES for quick resolution of any issues. Our Rancho Bernardo facility is the center of support for staff specifically assigned to support the County, and as the initial point of contact for the County for service. Other subject matter experts within our Identity and Access Management practice and portfolio virtual teams will also provide support and service as needed. The HPES Tulsa Data Center in Tulsa, Oklahoma will host the majority of County IT infrastructure and core IT services. This includes the infrastructure for ADFS, Oracle IDAM, and Active Directory. The HPES Continuity Services center in Colorado Springs is the designated disaster recovery (DR) site.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Key Processes

By incorporating the HP Global Method (HPGM) for Identity and Access Management, we will take an iterative approach, addressing issues and improvements in data quality and data management—in practice and in implementation. Through this process, we will work closely with the County data teams and other transformation, integration, and architecture (TIA) data architects to define and manage County IT outsourcing enterprise data semantics. HPGM for Identity Management advocates a rapid, incremental, and iterative approach that can be aligned with the County's hybrid development methodology of "AgileFall."

In addition to HPGM we will also use a standard TOGAF-based architecture approach to develop the solution artifacts and produce the required documentation to make certain that the solution is not only documented correctly, but will also minimize the overall implementation risk to the County. These methods will be integrated with the County's current Architecture and Solution Reviews in conjunction with the County's CIO office and relevant County Agencies.

For the Oracle IDAM Suite HPES will work with the current HPES IDAM architect to make certain that the design, development, and deployment of the Oracle IDAM Suite will follow standard Oracle design and deployment methods that will make sure that the Oracle platform will operate within the design parameters. Any significant design changes to the platform or changes to the Oracle Databases will follow Oracle-mandated practices.

The Computer Services Registration Form (CSRF) and process will be replaced to meet the requirement specified in Section 2.18.2.5 - Contractor shall develop automated workflows to manage access Service Requests. HPES will leverage the Oracle Identity Manager product to automate the Access Service Request process. Automation will include the ability to create a request with all appropriate validations, route it for approvals, email notifications, and predefined reports. The Oracle access request feature will integrate with the Service Portal as well as the automated provisioning capabilities that are specified in Schedule 4.3 Operational Services, Section 2.18.2.12. HPES will complete the workflow automation specified in Schedule 4.3 Operational Services, Section 2.18.2.5 during the transition period.

HPES recently presented County with a budgetary estimate for automated provisioning/de-provisioning of user identities based on human resource events via an interface to the PeopleSoft application. The budgetary estimate presented was broken into two phases based on HR use cases.

As part of transition, HPES will implement the first phase of the above referenced automated interface to the County PeopleSoft application. HPES will also implement second phase post-transition. If the County

decides to approve the budgetary estimate as part of the current information technology outsourcing (ITO) contract, HPES will adjust transition activity and pricing accordingly.

Any remaining requirements not currently in place will be included in the IAM roadmap.

- Automated Tools – Automated systems and tools involved in proposed solution

Our solution includes the following Oracle components that are already in use, as shown in Table 17.

Table 17. List of Software

PRODUCT	VERSION
WebLogic Server 11gR1 Generic and Coherence	10.3.5
Identity and Access Management	11.1.2.0.5
Identity Management 11gR2	11.1.2.0.5
Fusion Middleware Repository Creation Utility 11g	11.1.2.0.5
Enterprise Content Management 11g	11.1.1.5.0

- Qualifications and Experience – Background and experience in comparable environments

HPES has successfully deployed all of the major Identity Management elements currently running within the County, including Active Directory (AD), Active Directory Federation Services (ADFS), Oracle Identity Management Suite, Public Key Infrastructure (PKI), Office 365, and Digital Signatures. All continuing integration and design efforts for the County are being performed by HPES as well.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.13.1. Describe your proposed approach to develop an End-User account consolidation plan and End User Account Management Architecture.

We propose to develop an End-User account consolidation plan and management architecture as follows:

- Use the County Strategic Plan to provide the architecture vision for IDAM.
  - The County Strategic Plan is to build enterprise-grade identity and access. We are architecting IDAM to become a Zero Downtime Platform to serve the application community.
- Use the Oracle Identity Manager to manage all end-user accounts (expand existing capability).
  - Currently, the County relies on the Computer Services Registration Form (CSRF) process and manual administration to manage end-user accounts. We will build a capability into Oracle Identity Manager that will create network and email accounts automatically when a new employee joins the County. It will deactivate the accounts when an employee leaves, based on data fed from the County Human Resource System. We will build capability into Oracle Identity Manager so we can manage Service Provider accounts.
- We will utilize user data within PeopleSoft to manage the life cycle within the Oracle Identity Manager.
  - Use PeopleSoft to determine the life cycle of an ID.

    When a new employee joins the County, the Human Resources system will be the authoritative source for identity data. For the County, this is its PeopleSoft (PSFT) application, which will have a record for each employee. Oracle Identity Manager (OIM) will be integrated with PSFT, and

when a record is provided for a new employee then OIM will create accounts automatically in the County's Active Directory and Exchange environment. When an employee leaves the County, PSFT will indicate such activity. And OIM will inactivate the corresponding accounts in AD, Exchange, and other user stores. When an employee transfers to another department or business organization then OIM will receive notification from PSFT and take action based on established business rules. As the authoritative source of identity information, PeopleSoft will be the driver of any necessary actions by OIM, and the process will be automated with little need for manual administration.

- Actions taken on the County user accounts will be based on business rules established within the County such as hire, termination, transfers, leave of absence (LOA)/return from leave, and re-hire.

  As described above, PeopleSoft will be the driver of the actions taken by OIM. Although the actions taken by OIM will be triggered from PeopleSoft updates, the actions themselves will be directed based on business rules that can be integrated into OIM. For example, if the trigger from PeopleSoft is a transfer between one department to another within the County organizations then rules can be programmed into OIM that would disable access to one type of data and allow access to other data if that was the policy. In the case of a termination notification from PeopleSoft, OIM would disable Active Directory and Exchange accounts.

2.5.13.2. Describe your proposed approach to migrate all Portfolio Applications and cloud applications or services to the Identity Management Service

HPES proposes the following approach to migrate all Portfolio Applications and Cloud applications / services to the Identity and Access Management service:

- Make certain that all current County IDAM platforms are stable and expandable, and that they fit into the County's architecture vision for IDAM.

  Currently, we manually monitor logs from all components in the IDAM infrastructure. We plan to use Oracle Enterprise Manager to monitor the IDAM infrastructure. This will enable us to detect problems and resolve them in a timely manner—thereby enabling us to create a more stable IDAM platform.

- Reduce the number of accounts and passwords that the end user must manage, including web-based/standalone applications within the County and third-party applications (both cloud and SaaS based).

  By migrating more applications into the IDAM platform, more applications will leverage the Single Sign-On (SSO) capability in the IDAM platform. SSO enables users to utilize one user account and one password to access more than one application. With more integration into IDAM, the end user will have fewer accounts and passwords to manage. We are also building a Federation Identity Provider capability so that County employees can use their County Active Directory ID and password to access third-party applications in the cloud. This involves the following:

  - Institute an architecture principle in the design phase for every application to make use of the Oracle IDAM solution.

    A core principle in the architecture in the design phase of new applications will be to integrate as many applications into IDAM as practical—both to protect and build on the County investment in Oracle IDAM, but also to provide a consistent, easy-to-use end-user experience.

- Review all existing applications and services that require credentials to make certain that they are on a migration path to integration with the County IDAM solution, facilitating AD awareness—for example, UNIX, no local accounts on servers, and so forth.

  All applications and services that require credentials should be reviewed to determine if they can be integrated into the Oracle IDAM solution. Some applications may not be able to be integrated or may be too costly to justify, but each one should be evaluated so that the County can streamline access as much as possible. We will create a plan to accomplish all of the necessary integrations. Depending on the number of applications being integrated, the plan approach will likely be phase based because not all applications can be integrated at one time. HPES will work with the County to determine appropriate sequencing.

- With-cloud based applications we will establish a federation relationship with the cloud-based application provider to enable County employees to use their County credentials to log into cloud applications and services.

A Federation Identity Provider feature in IDAM will enable County employees to use their County credentials to log into cloud-based, third-party vendor applications.

2.5.13.3. Describe your proposed approach to integrate external constituents within the Identity Management Service.

HPES has proposed a Transformation project in Section 2.12 (response to Exhibit KK, Section 3.8) to implement Identity and Access Management as a Service (IAMaaS) to provide Identity Federated Services and add external constituents to the Identity Management service. IAMaaS is a cloud-based Identity and Access Management (IAM) solution built using the Computer Associates (CA) secure cloud product for multi-tenancy. IAMaaS is hosted on the HPE Helion Managed Virtual Private Cloud for U.S. Public Sector. A complete description of IAMaaS is provided in Section 2.12.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

It is also possible for the IAMaaS service to replace the Oracle Identity and Access Management suite to become a single-provider solution for both internal and external users of the service. The trade-off is that all of the work that has been completed to date in integrating the Oracle product set to the current Portfolio Applications would have to be reproduced using the new solution. We would need to do a more complete cost-benefit analysis to determine if this approach would be more cost-effective in the long term; we have chosen to leverage and augment the County's current investments in Identity and Access Management solutions rather than replace them.

Reporting Management Services (Sched 4.3, Section 2.19)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES understands that accurate and timely reporting is a critical component of the successful ITO delivery for the County. Well-defined reporting practices enable the County to make the critical, strategic, and financial decisions to keep their IT services running properly and respond to the needs of their employees and the community. The HPES and County partnership works to develop reporting strategies that keep their IT services up to date and the entire organization informed about the status and quality of the services provided by HPES. Near-real-time monitoring of vital touch points, often through dashboards, is important to capture and report on systems, frameworks, and operations priorities. HPES has a history of meeting and exceeding the County's reporting requirements. As such, we will continue to satisfy County reporting requirements as we work collaboratively to develop new reports and tools, including online dashboards.

Solution: HPES' solution and commitment will include the development, generation, and submission of deliverables defined in Exhibit L / Schedule 5 of the RFP. HPES knows the current reporting criteria and will continue the current level of reporting without interruption upon contract start. We will identify necessary reporting additions and enhancements to be completed as part of the overall cross-functional transition timeline. As part of the transition process for each framework, we will develop that framework's new report set (as identified in the RFP), either as a new report, or as an update to an existing report, where applicable. As the new reports are completed, we will begin posting them on the Service Portal. During the cross-functional transition, we will also implement Microsoft SQL Server Business Intelligence to begin the process of building a reporting data warehouse, thereby bringing more automation and continuous improvement to the reporting process.

While the initial focus will be on supporting SLA Reporting, the data warehouse will provide a central repository that will support other analytic scenarios as determined by reporting and County/Contractor quarterly review. We are committed to continuous improvement and, over time, we will work with the County to extend both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured in terms of a number of ways, such as, increased system availability, reduced system disruptions, predictive analysis of system changes, and optimizing staffing levels.

Specific areas of ITSM that can benefit from analytics:

- Service Strategy and Improvement Analytics: This area focuses on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis

- Service Design Analytics: We see this as a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data we can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.

- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

- Service Operations Analytics: Blending ITSM data and baseline IT performance data, Contractor shall conduct analyses to reduce business impact of events, incidents, and problems.

Post-transition, through a coordinated effort, HPES will identify specific subject matter experts for each reporting requirement and match them with a County counterpart to make certain that any new requirements are identified and supported for each of the Schedule 5 reports. In addition, HPES will demonstrate new and additional reports that the County may find valuable to manage their IT infrastructure, as well as streamline the reporting process as new transition and transformation tools are applied. The implementation of HPE Service Manager opens up a new chapter on the availability for new and enhanced reports. The County will have near-real-time reporting with fresh data to proactively monitor service performance and to take necessary actions. Service Manager provides 100+ out-of-box (OOB) reports; intuitive UI helps to create easily navigable role-based dashboards to show only what is applicable to a particular role. Each report has the option of printing and exporting (PDF, MS Excel, and HTML). Service Manager also has built-in reports for KPI reporting.

Rationale: HPES has a well-documented and dynamic reporting management operation established and in place. The rationale for our approach is to continue to provide a consistent, dependable reporting stream while using our subject matter experts and transformation tools to grow and enhance our reporting capabilities. Our hands-on experience and interoperation with the County informs our proven solution and

validates its continued usage. Our data analysts and cross-functional leadership are responsible for making certain that reports are generated accurately, on time, and in accordance with design or agreed-upon specifications. Moreover, our intimate familiarity with County needs and nuances enables us to work collaboratively to develop and maintain meaningful reports and dashboards.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The County will continue to receive the current reports during the transition period. We will work with the County to consider new and improved reports through conducting workshops and meetings for the County to consider modifications to existing reports or to make new reports. These collaborative sessions will be conducted by HPES resources at our facility in Rancho Bernardo or at County sites identified by our customer.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES will provide to the County all reports outlined in the RFP via the Service Portal. We will provide these reports and track the usage to provide feedback to the County on reports in high demand and those that potentially could be modified to provide additional value or possibly sunset. HPES understands the County's evolving requirement for improved or enhanced reporting processes and will update processes accordingly and as needed to reflect changing needs in this area.

As previously noted, we will create an analytics and reporting data warehouse during the transition period, based on MS SQL Server Business Intelligence, to facilitate ongoing automation and continuous improvement in efficiency and quality of our reporting capability.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES uses multiple tools and data extract processes in the course of producing reports. There are also numerous tools used as data sources, such as Service Manager, myRequests, iTrack, and many others that are not listed here. The appropriate tools and products to be used in producing each report will be finalized during the transition period, but will consist of, at a minimum:

- Microsoft SQL Server Business Intelligence
- Microsoft SharePoint
- HPES End User Access (Service Portal)
- EMC Documentum (DocVault)
- Various scripts and development tools, as appropriate

- Qualifications and Experience – Background and experience in comparable environments

HPES provides Report Management for the following clients

- City of Anaheim
- Kraft Food Services
- General Motors
- Proctor and Gamble
- SOMS

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Domain Name Management Services (Sched 4.3, Section 2.20)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Solution: The request for a new Domain Name (DN) and add-on DN services is initiated by the County point of contact (POC) via an IMAR request to the HPES Service Desk in myRequests or a project requirement. The Domain Name Administrator (DN Admin) will treat either request as authorization to purchase the DN and DN services from an accredited registrar/vendor.

The HPES Service Desk routes the IMAR request to the DN Admin, who takes the following actions:

- The DN Admin checks the DN Portfolio for an existing account for the requesting department. If the requesting department has an account then the DN Admin uses the existing account for purchase or creates a new account if one does not exist.
- The DN Admin saves the confirmation receipt for future reference and adds DN and DN services to the DN Portfolio in the Integrated Asset Management System (IAMS).
- The DN Admin then emails the County POC the confirmation of purchase and gives the County POC an initial username and password.
- If the requested DN is not available, the DN Admin will email the requestor for an alternative DN.

The DN Admin is responsible for (1) actively monitoring the renewal of DN and associated DN services and (2) acquiring approval from the County POC for renewal. The DN Admin takes the following steps for renewal:

- The DN Admin emails the County POC about DN renewal approximately 30 days before the expiration date. If there are DN services associated then the DN Admin will also request DN services renewal.
- The County POC responds with approval to renew the DN. If there are DN services associated, the County POC will also indicate whether or not to renew the DN services.
- The DN Admin pays renewal fees to the accredited registrar/vendor for the DN.
- The DN Admin updates the expiration date on the DN Portfolio accordingly and enters it into the IAMS.
- If the County POC decides not to renew the DM then the DN Admin will update the DN Portfolio in the IAMS.

The County POC may request cancellation of a DN and associated DN services prior to its expiration. The DN Admin will treat these requests as authorization to release the DN and associated DN services. The following are the procedures for cancellation of a DN:

- The County POC submits an IMAR-Remove ticket in myRequests.
- The Service Desk routes the IMAR-Remove ticket to the DN Admin.
- The DN Admin cancels the DN and associated DN services with the registrar/vendor, removes the DN from the DN Portfolio, and saves the documentation in the IA.

The DN Admin minimizes the number of registrars/vendors from whom they purchase DNs for ease of management and transition of services. The DN Admin purchases/renews DNs for no more than a 1-year subscription to minimize the cost to the County in the event that a cancellation occurs. We will consolidate domain names to only accredited registrars, as each DN comes up for renewal.

The DN Admin will create an Annual Domain Name Management Plan that details all DNs in the DN Portfolio, expiration dates of existing DNs, and any changes in DN management procedures. The DN Admin will also create and post to the Service Portal a monthly report that will include the following:

- Domain Name
- Total quantity of managed Domain Names
- Quantity of new Domain Names added in the last month
- Quantity of Domain Names retired in the last month
- Quantity of Domain Names retained by the County
- Summary data for each Domain Name:
  - Domain Name ID
  - Type/extension
  - Renewal date
  - High Org
  - Low Org
  - County POC name, email, and phone
  - Secondary County POC name, email, and phone.

Many DNS hosting services do not distinguish between the purchaser and the administrator of the services. In these cases where the purchaser and administrator are one account—and where the County is using additional services, such as web hosting or file sharing—HPES assumes these are out of scope as is the current practice until such time as HPES is authorized to purchase on behalf of the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Domain Name management will be performed by HPES' Domain Name Administrator, who will reside in HPES' facility in Rancho Bernardo.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

We will conduct the Domain Name management in accordance with the agreed-upon Domain Change Management process with the County. We will implement continuous improvement in accordance with the HPES ISO 9000-certified processes and our adherence to ITIL processes for service delivery, including the review, analysis, prioritization, and recommended improvement opportunities.

- Automated Tools – Automated systems and tools involved in proposed solution

The Domain Name Portfolio will be stored and continually updated in the Integrated Asset Management System.

- Qualifications and Experience – Background and experience in comparable environments

HPES has detailed understanding of the County's Domain Name processes and procedures. HPES, along with the County, developed this process and has been successfully performing this for approximately 4 years.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None at this time.

2.5.14 Business Analyst Services (Sched 4.3, Section 2.21

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Solution: The business analyst is one of the most critical roles in the requirements management process. As such, the HPES solution includes establishing a team of business analysts to act as liaisons to the County business groups, including LUEG, CSG, FG3, PSG, HHSA, and the Enterprise. These analysts will gather, analyze, communicate, and validate requirements related to new IT projects or changes to existing applications, processes, or policies. The HPES business analysts will engage all County and HPES stakeholders as well as contractor roles across the applications, engineering, testing, end-user support, and security towers. Our solution recognizes the complexity of this role and provides tools for multifunctional teams.

The business analyst articulates the County's high-level requirements for an IT system and supports development of those requirements for consideration within the scope of new development efforts. To do this, we will work closely with the County business owners and users. Business analysts have an advanced level of knowledge and expertise within the particular industry or client they support. We will field a mix of experts who know the County's business well and are strong in eliciting and documenting requirements. This hybrid approach to staffing the Business Analysis Center (BAC) gives the County the optimal mix of knowledge of your business and functional/technical expertise from outside the County. The benefits of our implementation of the BAC include:

- Flexibility in the business analyst staffing arrangement. - Analysts will be available through a pool of resources the County can use on request or exclusively for specific projects or objectives.
- Shorter delivery time to meet customer demands. - As the County has direct contact with HPES business analysts that can act as a bridge between requirements definition and solution development, it can improve and enhance service delivery to its employees and constituents.
- Experience in aligning the right resource to the right effort. – Previously, the County had experience with Customer Solutions Advocates (CSAs) who were dedicated to County business groups. CSAs had intimate knowledge of the business groups to which they were assigned and provided business analysis services to these groups in solutioning and assisting in solving business problems. While our solution for business analysis focuses on the identification, training, and development of experienced business analyst professionals, the CSAs are highlighted in the Qualifications and Experience section of this proposal as examples of how HPES understands how to deploy effective personnel to impact quality delivery.
- Quality and standardization in requirements identification and development. – As part of the BAC, each analyst will benefit from a common set of industry standard best practices as defined by the BAC and approved by the County. These processes will not only define behaviors and methodologies for assisting the county to develop the quality SOWs and requirements documents that are necessary to expedite project outcomes but also to create a smooth transition from identification of business needs through the project request process, requirements development, and beyond.
- Continued engagement throughout the project life cycle. - Business analysts will participate in post-requirements phases, for example, guiding user acceptance testing and acting as training and documentation SMEs.

To support the solution, HPES will leverage our Enabling Delivery and Global Excellence (EDGE) methodology and toolset to develop the standard processes the team will follow. EDGE is a repository of

best multifunctional methods, tools, and processes that will inform the creation of a custom, repeatable solution that is right-sized for the County.

Rationale. HPES' current executive leaders are advocates of continued and expanded business analysis support. We welcome the opportunity to provide that expanded support.

Based on our experience and our knowledge of the County business, the ideal business analysis services for the County should meet the following objectives:

- Support the County by increasing the maturity, consistency, cost-effectiveness, and overall business value of business analysis services by developing a BAC
- Provide the right mix of County business knowledge, technology expertise, and business analysis expertise
- Provide a methodology and tools with flexibility for all types of projects, regardless of size or complexity
- Provide access to embedded business analysis resources via the BAC
- Provide portal-based access to a business analysis methodology tailored for the County
- Assist with business analysis training for County users via the BAC. This training will be focused on project-specific needs
- Keep all processes lean and responsive to the County without over-proceduralizing business analysis to allow for expedited delivery
- Provide business analysts with the right aptitudes, certifications, and ongoing training.

This is a Gartner mode 1 approach appropriate to the type of development HPES does today. The County may want to advance toward mode 2 techniques. If the County desires to augment the BAC with mode 2 analysts, we will work with stakeholders to identify a candidate project to establish and prove the approach, and will add mode 2 methodologies and touchpoints to our process repository for the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The way in which an organization defines and delivers requirements is imperative to the success of an IT project and, in turn, to the success of the business function supported by that project.

Defining and managing requirements well can be a difficult task. Requirements emerge from an idea or as a business initiative, evolve through the definition phase, and often change in the delivery phase. The many people and groups involved throughout the requirements development and solution life cycle must collaborate and communicate clearly. The adoption of Agile and other rapid methodologies across the County makes defining and managing requirements even more important.

HPES will provide a pool of business analyst resources to be guided by common and flexible best practices and tools, which will improve the quality standard for requirements gathering. In the past, the County has used embedded resources to understand the business and craft appropriate requirements.

HPES will be flexible when assigning the work locations of all analysts to meet the needs of the projects and departments. Analysts will be located in either the HPES Rancho Bernardo facility or an embedded location within the County. If a County department wants a dedicated resource, we have that flexibility and will work with the County to identify the best resource and solution.

Following our flexible, hybrid approach, we will provide an opportunity for current business analysts to gain more training and certifications as part of their professional development. We will develop our team's talent and enhance staffing where necessary to meet the County's needs. Our approach provides the right mix of skills and experience to build high-performing teams and will promote the BAC's

success. In addition, we will require specialized business analysis training, experience, and certifications when engaging new talent. Incoming business analysts will demonstrate at minimum:

- Business- and technology-related education and experience
- Professional experience performing business analysis services
- Exceptional communications skills and strong interpersonal skills, including structured and unstructured facilitation
- Ability to understand and document functional business requirements and to translate business requirements into technical requirements and/or solutions
- Experience with formal business analysis methods and tools
- International Institute of Business Analysis (IIBA) Certified Business Analysis Professional™ (CBAP) certification or similar is a plus.

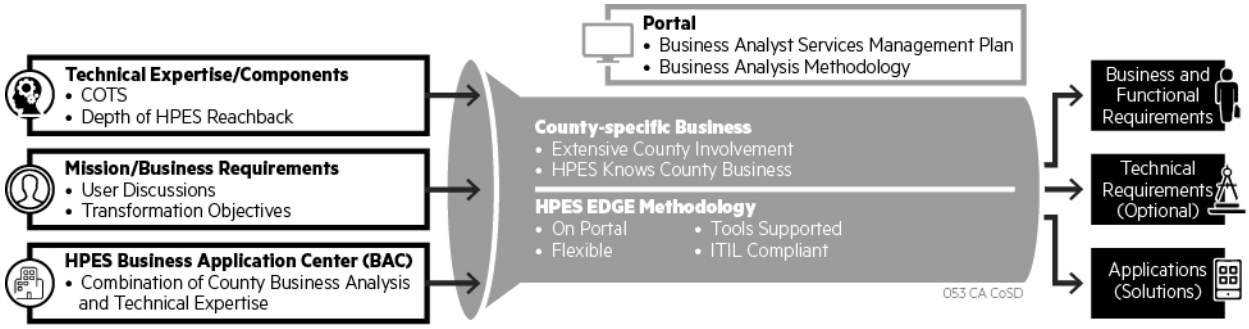
- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

One of the keys to developing applications that meet business requirements is to define the right requirements up front. Requirements must be clear and succinct, and they must incorporate feedback from multiple stakeholders. Using enterprise-level and project-level best practices in defining and managing requirements makes sure that projects address their intended business need.

As cloud, mobile, and composite applications bring even greater complexity to the requirements process, they also bring the County the opportunity to reduce customization and deployment times. With business analysts working with the County to identify its rapidly shifting business needs, HPES will expand its use of Agile development techniques to drive improved delivery and user satisfaction.

Our methods, processes, and tools include HPES' EDGE, the cornerstone of our standardized delivery, enabling our global applications services teams to operate consistently with a high level of quality and efficiency. It encompasses all the standard processes, tools, and accelerators that our Applications Portfolio global experts endorse and deploy to the field. Our use of EDGE as the starting point for County process development will inform the creation of a custom, repeatable solution that is right-sized for the County.

Figure 29. Business Analysis Solution



Our comprehensive approach to business analysis services embeds best practices while remaining flexible.

The EDGE methodology aligns with PMBOK, ITIL, and CMMI standards through a standard set of tools and processes that can also be customized to fit the needs of the County. Via EDGE, HPES implements best practices—at both the enterprise and the project levels—to capture and manage well-defined application requirements. These practices help teams that use flexible and streamlined iterative processes, as well as those using traditional waterfall methods to succeed. Overall, improving requirements

definition and management processes can help the County reduce the time required to deliver solutions and increase the likelihood of their success. We will publish a County business analysis methodology on the Service Portal and use the BAC to help use and extend best practices throughout all County projects.

Enterprise-Level Best Practices

Our first three best practices are implemented at the enterprise level. Through enterprise-wide standardization, a common language, and traceability, the County can create well-defined requirements that provide consistency throughout the application life cycle and become part of the County culture.

Enterprise-wide standardization - By standardizing requirements management at the enterprise level, the County can promote collaboration and eliminate silos between business analysts, development, and quality assurance (QA). A single system for complete requirements management provides the most up-to-date information for project teams. This is particularly important as requirements change over time, either because of changing business conditions or by design as part of an iterative development process such as Agile. A single requirements management system also enables better oversight.

Common language - Providing consistent guidelines for the language used for all requirements makes requirements easier to write and follow. This prevents both the overwork of adding more detail than necessary and the extra time needed to cycle back for more information when descriptions are too vague.

HPES recommends guidelines that call for:

- Using simple, imperative sentences
- Using the present, indicative tense; in other words, consider adding an "s" to the verb (for example, the system requires a single sign-on).
- Avoiding semicolons or conjunctions (and, or). Keeping one requirement per sentence makes it easier to measure and delegate development and testing work.
- Avoiding "can" or "may" statements. Requirements using these verbs will be too vague.

Following these guidelines makes the requirements more robust and easier to follow and enables measurement of their quality.

These quality metrics include:

- **Lines of text**—the number of lines of text in the requirements document. When there is uniformity in the way requirements are described, this metric allows the user to estimate the functionality and degree of testing required for the software.
- **Imperatives**—the number of imperatives in different categories, such as "shall," "must," and "will." This number gives a rough estimate of the degree of design functionality required in the software. It also gives an estimate of the degree of testing required to satisfy these imperatives.
- **Weak phrases**—the number of weak phrases such as "large," "fast," "enough," etc. Weak phrases indicate vague design requirements that are non-testable.
- **Completeness**—the percentage of requirements that do not contain phrases such as "TBD" (to be determined) and "TBS" (to be specified). Requirements containing these phrases are considered incomplete.
- **Option phrases**—the number of phrases such as "can," "may," "I/we think," and so forth. These indicate requirements that might be difficult to satisfy in development.

Another best practice to encourage the use of a common language for requirements is to provide a template or set of templates for requirements definition.

Traceability - It is important that we enable traceability throughout the application life cycle to determine whether a project meets requirements. The ability to bi-directionally trace links between requirements and

tests, as well as between requirements and code, allows business analysts and other stakeholders to make sure that IT delivers what the business expects.

Traceability makes requirements the basis for testing the application, which enables the QA team to test against criteria defined by the business. For developers, requirement-to-code traceability enables opportunities for reuse if similar functionality is needed across different applications. For the QA team, traceability ensures a record of test case coverage associated with business requirements, which is essential for defect reporting. And for County managers and executives, traceability provides visibility into the progress metrics that matter most—how well the application meets the needs of the business.

Traceability metrics include:

- Requirements traced —number of requirements traced to or from each specification
- Requirements untraced—number of requirements that are not traced
- Requirements inconsistently traced—number of requirements inconsistently traced
- Linkages—number of upward and downward linkages for each requirement. This helps determine reuse and the impact of changes on the overall application
- Coverage—percentage of requirements traced to passed tests, failed tests, or tests not run.

Project-Level Best Practices

The next four best practices occur at the project level. Adopting these practices brings clarity to the requirements process and helps eliminate rework in application development and testing. In addition, these steps help eliminate overwork and rework in the requirements definition process itself.

Be lean. Do not create requirements assets unless they will provide value to the application team. The assets with the most value will be the ones that can be reused. A lean approach includes automating processes and eliminating waste. By systematically organizing requirements, it becomes easier to see which requirements are needed and which can be eliminated. Standardizing the content of requirements—with templates and a common language—helps make requirements easier to understand and eliminates rework.

Iterate. Create requirements iteratively to generate feedback, promote collaboration, and enable teams to identify defects early in the software development life cycle. A best practice is to start with a high-level business requirement by describing who needs the functionality for what purpose and why. Then, rather than working in isolation, the business analyst writing the requirement should gather feedback from major stakeholders on whether the high-level requirement adequately describes the business need. Developers should also provide feedback on whether there is enough information to begin coding. If not, the business analyst should drill down to add more detail. If there is enough information, the developers can get started.

Different requirements will require different levels of detail. The County can save time and reduce complexity by providing just enough elaboration. There is no need to over-describe requirements that are easily understood.

Requirements assets that can be reused, such as business process models (BPMs) that can be used to generate requirements, provide the most value.

As a project goes through iterations of requirements definition, it is important to measure where and how requirements change over time. Change metrics include:

- **Volatility**— number of requirements added, deleted, and modified, classified by a reason for change.

- **Initial allocated requirements**—number of technical and nontechnical requirements originally provided by the customer. This metric, along with final allocated requirements and changes per requirement, describes how much requirements change.
- **Final allocated requirements**—number of technical and nontechnical requirements that were used to build the final software product.
- **Changes per requirement**—number of changes made to each requirement.
- **Changes over time**—number of changes per week, for example. This describes the degree of requirements volatility. This number should decrease towards the end of the software life cycle, indicating convergence of requirements.
- **Cause of change**—categorizing the cause of changes helps in identifying the most common reasons for change and can be used to improve the software process.
- **Source of change**—identifying the source of change (that is, who requested the change) helps anticipate the sources for change in the future.

Visualize. We can use visualization to increase understanding of requirements and the dependencies between requirements. Visualization makes it easier to identify potential problems, such as missing use cases. And pictures can be easier to read and navigate than text-based requirements. For teams that do not want to follow the Agile practice of writing code early in the process, visualization and simulations can be used to elicit early feedback to achieve many of the same objectives.

Collaborate. Collaborate and break down silos between groups from the beginning of the process. For instance, while a business analyst might have the end user view of what a requirement should be, collaborating with the development team will help determine whether implementation of the requirement is feasible.

When these best practices are implemented, our projects are more likely to meet intended business metrics, including budgets, schedules, and client satisfaction by eliminating the gaps between work processes performed in IT silos.

Standardization and Best Practices.

Embedded in our methodologies are common best practices that can be tailored to suit the County's needs, including those from BABOK, CMMI, ISO, and SSE. These methodologies integrate business analysis with the other development disciplines to verify continuity of standards through the project stages.

- Automated Tools – Automated systems and tools involved in proposed solution

To ensure excellent business outcomes, we must address the need for better requirements. The right requirements management solution will facilitate the management of the requirements life cycle. Our methodologies meet the necessary requirements:

- Be easy to use
- Facilitate a single "point of truth" for both visual and textual requirements
- Support collaboration between stakeholders to ensure the right thing is being captured
- Provide traceability between requirements and other development assets (test, defects, code, and the like)
- Enforce standardization to ensure consistency and quality between requirements

Our business analysts will pick the right tool or tools for the job from a consistent set of best-in-class tools, including those listed in Table 18.

Table 18. Business Analyst Tools

TOOL NAME AND VENDOR	DESCRIPTION	VALUE-ADD OR TAILORING FOR THE COUNTY
HPES EDGE	• Flexible repository of methods and tools to support business analysis • Supports entire life cycle through test and deployment	• Integrated modules support our ITSM compliant procedures • The capability to manage services using a lifecycle approach, with consistent improvement built into the governance model, allows IT to truly enhance the value to the business
ProVision	• Enterprise and business architecture software tools	• Depth of modelling tailorable to project
Borland Together®	• Visual modelling	• Depth of modelling tailorable to project
HPE Agile Manager	• Integrated part of HPE tool suite	• Rapid project development • Incremental user validation of product functionality
HPE Project and Portfolio Manager (PPM)	• Integrated part of HPES tool suite	• Agile project-level and portfolio-level management tools
MindMeister	• Online mind mapping tool that enables users to capture, develop, and share ideas visually	• Visually capture business requirements without excessive process • Quickly gain user approval of functional requirements

- Qualifications and Experience – Background and experience in comparable environments

HPES is experienced with business analysis on County projects and on other ITO projects.

HPES has already provided business analysis services support to the County. These examples demonstrate our understanding of the County's business needs and how our methodologies and support can flex to support the County at the department level and throughout the enterprise.

In 2013, an HPES business analyst and customer support representative helped the County implement mobility and tablet use for inspection services applications.

Prior to the Notice of Decision (NOD) approval, County policy prohibited the connection of non-standard computing devices on the network. Additionally, there was not a standardized process by which non-standard devices could be reviewed for approval so that they could be evaluated on the network on a temporary basis. This capability would assist with procurement decisions. This issue in particular affected LUEG-DEH and AWM as they looked for a form factor that met the mobility business needs and use requirements of their inspectors. But soon other business groups, such as HHSA Public Health Nursing and PSG Public Defender and Office of Assigned Counsel, became interested in using a smaller form factor device in performance of their duties. The County was transitioning from a "sitting and typing" to a "walking and collecting" type of work style.

DEH created and formalized a mobile hardware committee to gather, identify, and understand business requirements for the computers used in field duties and inspection data collection. Ultimately, these requirements served as the basis for identifying the best possible hardware candidate devices.

This project used a process tailored for the County and took several months. CSAs/business analysts worked with the County departments to understand:

- Tasks accomplished during the inspection process
- Tools or resources that an inspector has to accomplish inspection tasks
- Environment in which inspection tasks are accomplished

Additionally, CSAs/business analysts helped to:

- Define and translate business to technical specifications
- Develop a scoring and weighting rubric
- Determine workplace and environmental conditions and factors, including
  - External keyboard
  - External mouse, mobile printer, and portable scanner capability as a peripheral
  - Use while standing/walking
  - Sunlight readable display
  - Brightness adjustment
  - Screen contrast.

Table 19. Qualifications and Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND HOW IT IS RELEVANT TO THE COUNTY
County	HPES has strongly advocated the value of business analysts at the County We previously fielded embedded resources in several County divisions Through our IT teams and daily interaction with the County from top to bottom, we are knowledgeable of the County's business and mission
HUD HITS	Our business analysts helped assess and implement a mobile housing inspection application
Navy Selection and Classification (RIDE Web Services, Fleet RIDE Development, Deployment, Sustainment, and Enhancement)	HPES provided a consistent methodology for the U.S. Navy's Selection and Classification (S&C) process transformation. HPES used the IDEF0 activity modeling technique to develop the functional view of Navy S&C processes. To expand Fleet RIDE to support the Naval Selected Reserves, HPES coordinated with Navy S&C stakeholders and a "Council of Captains" and obtained consensus to define "to-be" business processes and developed a process improvement roadmap.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

2.5.14.1. Describe your proposed approach to gather and document County business functional requirements when working with County departments.

As described in 2.5.14 on Business Analysis Services, HPES will leverage our Enabling Delivery and Global Excellence (EDGE) methodology and toolset. EDGE is a flexible repository of best multi-functional methods, tools, and processes that we will tailor for each County project.

Our approach to Business Analysis Services relies on a set a proven best practices, but is highly flexible for the County. We will draw on a pool of business analysts who have a mix of experience and diverse technical expertise and functional knowledge of the County and its businesses. The analysts will work directly with the County user groups to accomplish the following:

- **Gain Broad Involvement**. Review documented high-level requirements with internal stakeholders, including representatives of those capabilities who will be responsible for delivering the solution.
- **Define Goals and Requirements**. Confirm that defined detailed requirements support the business goals and provide compelling business value. Reconfirm boundaries for: business functions, current systems, internal and external interfaces. Confirm stakeholder and user profiles, business processes, user interfaces and use cases, interface requirements, business rules, data entities, non-functional requirements, geographic regions, language/culture considerations, volumetric(s) (e.g., how many reports were anticipated), and documentation.
- **Define Scope**. Identify perceived gaps in boundary definitions as issues. Document questions and assumptions with regards to understanding the high-level requirements. Transfer knowledge of detailed requirements and estimating assumptions (if any) from solution architect to business analysts and project team.
- **Use Leverage**. Leverage the experience of the detailed requirements development team and transfer knowledge to the solution delivery team. Review assumptions and constraints. Identify perceived barriers to evolving the detailed requirements into a solution. Confirm common understanding of the detailed requirements with client stakeholders. Review and discuss gaps, issues, questions, concerns, and assumptions.
- **Build Consensus**. Determine if the client and project manager agree that the detailed requirements are sufficient for solution development. If the detailed requirements are not sufficient, work with project leadership to assess the impact of delays resulting from rework of the high-level requirements. Raise requests for change as needed
- **Document Results**. The output of this work is a Business Functional Requirements Document. Once the functional requirements are agreed on, documented, and approved by the County, they can be translated into technical requirements or directly into a solution depending on the complexity and functional nature of the requirement. We will use templates that are already in use with the County and supplement them as needed with best practices templates from EDGE.

With this process and approach, the County users are involved every step of the way and own approval of the final Business Functional Requirements Document as the baseline for next steps in implementing a solution.

5.14.2. Describe your proposed approach to translate business requirements into solutions or technical requirements.

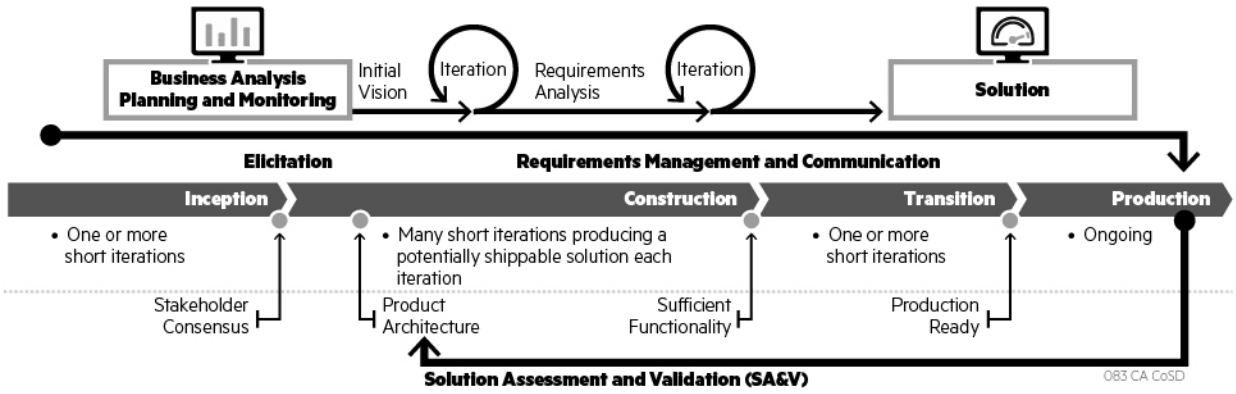
This approach starts with the Business Functional Requirements Document. Our proposed approach is:

- Review Functional Business Requirements and confirm joint understanding of the requirements (this process is streamlined and low risk if HPE business analysts helped develop the functional requirements.
- Assess functional requirements and technical components required to meet requirements
- Map all functional requirements to technical requirements

- Ingest and consider technical alternatives and review with the County
- Make build versus buy decision and gain County approval
- If Build, then follow development life cycle and build out technical specifications
  - Decomposition
  - Documentation
  - Requirements traceability
- If Buy, then perform COTS selection mapping capability to requirements
  - Select COTS
  - Create request to purchase
  - Follow OIC process
- Iterate technical specification and solution versus functional requirements to optimize business case – discuss tradeoffs with users and gain their approval
- Perform SIT and UAT
- Deploy

HPES has a comprehensive process for this translation and solution development, as illustrated in Figure 30.

Figure 30. Process to Translate from Requirements to Solution



Providing a streamlined approach to reach a solution provides sufficient process control to achieve success.

Additionally, we use the following best practices when translating requirements into solutions:

Once requirements are developed and refined, HPES and the County will also conduct a Build versus Buy Analysis that identifies a "best-fit" solution based on requirements and budget. The best return for the County comes when business requirements, staffing, and technology are optimally aligned with both user and mission needs. The business analyst's job is to analyze needs, document requirements, and identify optimal solutions.

Build. We will execute the requirements elicitation approach identified in planning until sufficient information is gathered to document the detailed requirements and estimate the cost to build. This cost can be compared to cost to buy COTS, and a final build versus buy decision is made. We will refer to previous iteration/release documentation as needed to shape the scope of the detailed requirements elicitation.

Depending on the nature of the build, we will decompose high-level information; abstract low-level information; distinguish requests versus needs; and distinguish requirements from design constraints. Identified requirements will include functional/system requirements and may include non-functional

requirements (such as performance, environmental, security, etc.), service-level requirements, quality requirements, and project management-related requirements deemed critical for project success.

Finally, we will store the collected information (such as informal or formal documents, meeting minutes, interview notes, emails, and other similar items) in a repository for future reference. We also will document the decision criteria and justification for selecting the build option. We will select a build process, which will lead to a build or development phase.

Buy. A COTS solution may be the lowest risk and least costly way to meet user functional requirements.

First, we will validate high-level requirements against the selected COTS product and perform a detailed assessment of the gaps to confirm that the essential requirements can be met (out-of-the-box, by configuration, or by customization). Business analysts will be trained in the use of the selected product (including the features, flow, and architecture) or we will include COTS SMEs in the elicitation activities to clarify how the COTS product can meet the requirements or the impact of potential customizations.

Next, if a COTS product is selected as part of the solution, we will conduct a day-in-the-life (the 'as-is' process) walkthrough to elicit detailed requirements and to identify essential customizations. The objective is to take the fullest advantage of the COTS functionality.

It is important to manage scope of solution and moderate user expectations during requirements elicitation. If a requirement is identified that appears to be out of scope, we will add it to the backlog list for future consideration, or follow the normal change procedure to change the scope before accepting the requirement.

Finally, we will store the collected information (such as informal or formal documents, meeting minutes, interview notes, emails, and other similar items) in a repository for future reference. We also will document the decision criteria and justification for selecting the buy option.

2.5.14.3. Describe your proposed approach to ensure Business Analysts have the necessary level and type of expertise to perform functional responsibilities.

Our approach to ensure that business analysts can perform successfully for the County has four elements:

- Recruiting and Hiring.
- Professional Development.
- Coaching and Feedback.
- Ongoing Experience and Professional Development

We provide details on each of these elements below.

Recruiting and Hiring. As a Tier 1 IT services company, HPES attracts the best talent. We offer all employees exceptional benefits and work challenges to fuel their careers. Because we are such a product-agnostic technology company, we attract business analysts who want to work with the best technologies from across the market.

When we hire new business analysts, we will put a higher premium on specialized business analysis training, experience, and certifications than on people already assigned to an account, like the County. Among the requirements for a business analysis new hire are:

- Business- and technology-related education and experience
- Professional experience performing business analysis services
- Exceptional communications skills. Strong interpersonal skills, including structured and unstructured facilitation

- Ability to understand and document functional business requirements. Ability to translate business requirements into technical requirements and/or solutions
- Experience with formal business analysis methods and tools
- IIBA Certified Business Analysis Professional™ (CBAP) certification or similar.

Professional Development. To execute HPES' strategy and achieve superior business results, we need strong leadership at all levels of the company. Key Talent @HPE is an intensive leadership development program designed to provide an exceptional, multifaceted, and focused development experience for high-performing leaders at HPE. We designed our tiered program to target different levels of leaders from executives through first level managers and high-level individual contributors.

Key Talent @HPE is designed to increase HPES' competitiveness by:

- Growing and retaining top talent
- Increasing the pipeline of leaders ready to assume more senior and/or critical roles
- Contributing to HPES' goals of leadership capability and diversity
- Delivering business value to HPES and our clients.

Participation in the tiered programs is on a nomination basis and participant selection is determined by annual talent reviews and performance assessments. The Key Talent @HPE programs involve structured development experiences that feature action learning, executive interaction, and personal and group development activities.

HPES recognizes that retention and development of human resources is essential. HPES knows that it is critical to retain current County resources with specific application and County business knowledge, while working to expand and improve these resources. Retaining motivated employees is key to effective management. Employees engaged in their work, satisfied with their environment, and focused on personal development prevent cost and productivity losses associated with employee-initiated attrition. We work relentlessly to make sure we have the most competitive, committed, and innovative workforce in the world.

Technical development and career ladders have similar support and follow similar approaches.

Coaching and Feedback. Nothing is more valuable to employee development than ongoing assignment-specific coaching and 360 feedback. Our County leadership has been in place for years and knows the County well, so, our business analysts become very effective very quickly on County projects. While our team has well-defined roles and responsibilities, we have a collaborative and supportive culture. All employees receive formal feedback on their performance and ongoing feedback and coaching on how to maximize their job performance. Our current leaders in Applications and the PSO will be invaluable in helping to optimize the performance of our business analysts.

Ongoing Experience and Professional Development. Involved throughout the development life cycle of the County's system, an HPES business analyst elicits and analyzes requirements, documenting the County's "to-be" state through technology-neutral models that represent the County's business organization, processes, data, and applications. Where appropriate, the business analyst applies reusable components (for example, COTS applications and industry framework models) as part of the solution. After establishing a requirements baseline, the business analyst shifts focus to managing the requirements, verifying their fulfillment, and developing user documentation and training.

Our business analysts apply several key elements to deliver consistent, high-quality requirements analysis:

- Proven global processes and techniques
- Specialized training and skills

- Standard tools supporting business process modeling, requirements management, and Unified Modeling Language
- Metrics-based process monitoring and improvements
- Reusable templates and examples
- Coordinated sharing of lessons learned and best practices
- Integration with companion capabilities
- Requirements quality testing (validation and verification).

Table 20. highlights the methods, industry standards, tools, and training we use to provide thorough, reliable business analysis.

Table 20. Business Analysis Capability Details

BUSINESS ANALYSIS CAPABILITY DETAILS	
Methods	• Requirements determination process • Requirements implementation risk analysis • Ambiguity analysis procedures supplied by the Quality Assurance and Testing Capability • Functional modeling supplied by the Quality Assurance and Testing Capability
Industry Standards Alignment	• We encourage business analysts to pursue the International Institute of Business Analysis (IIBA) Certified Business Analysis Professional™ (CBAP) certification. HPE contributed to the creation of the Business Analysis Body of Knowledge® (BABOK), skills competency model, and CBAP™ certification exam questions.
Tools	• ProVision • Borland StarTeam® • Borland Together®
Training	• A full curriculum of training courses and activities covering business analysis theory, tools, methodologies, and IIBA certification

Through consistency in our processes and diversity in our projects, our business analysts gain growth and experience opportunities they cannot obtain elsewhere. This helps in retention and in the professional development of our business analysts.

Chief Technical Architect (Sched 4.3, Section 2.22)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Implementing integrated information technologies to execute the County's strategic plan requires continual planning and methodical implementation of technology roadmaps and processes across all disciplines of the architecture services framework. This is critical for future success. As a continuum both from top-to-bottom (strategy to technology) and end-to-end (advise to manage), architecture must be an integral part of every County strategic initiative, not a standalone practice, a point solution, nor a discrete event. During the past 5 years, HPES played an integral role in architecture governance, which is "management" with the County. We have an in-depth knowledge of how enterprise architecture (EA) services impact the County's mission and consider these services as a key enabler and driver to move the County forward.

> Gartner observes that HPES' EA program is the "foundation of Transformation planning. It (HPES EA) views EA as a business-enabling continuum—from top-level business architecture (BA), through the different viewpoints of EA (for example, IA, SA and TA), and down to the programs, projects, and initiatives that enable targeted business outcomes."
>
> *Gartner Magic Quadrant for Enterprise Architecture Consultancies*

Rationale: HPES sees the Chief Technical Architect (CTA) as a key role in the architecture continuum, specifically being responsible and accountable to lead the development and delivery of strategic technology solutions that fit the business' needs.

HPES sees architecture as a seamless whole—from high-level enterprise and business architecture to the specific, detailed solution and technology architecture. We design everything in our architecture services around that unique vision: our methods, architecture profession programs, trainings, standards, and support process, among others. We architect to make things realistic and reasonable by applying our EA skills and principles to enable business capabilities, processes, applications, infrastructure, people and governance to meet today's challenges and those in the future.

We use a straightforward methodology, illustrated in Figure 31, based on recognized and proven Open Group practices (HPES RightStep, IT Solution Architecture [ITSA] and The Open Group Architecture Framework [TOGAF]) to engage with the County on these fundamental enterprise and business architecture issues. EA, done right, enables change and transformation while serving as the linkage between the County's key stakeholder groups, including business leaders, IT leaders and architects, and HPES. Well defined, it provides the foundation for solutions and alternatives based on the County's enterprise architecture.

Figure 31.. HPES' EA Methodology

HPES' approach enables change and transformation and provides the linkage between key stakeholder groups including business leaders, IT leaders and architects, and HPES to achieve business transformation.

Our EA methodology is end-to-end and business outcome driven. Unlike that of a traditional architect that designs a house and then leaves, ours is akin to one where the architect designs, builds, and then lives in the same house and continues to make improvements. This is how we help customers achieve their goals, and continue to monitor and improve on what we deliver.

CTA shall provide architectural and technical leadership, oversight on all projects and develop a set of cognitive roadmaps to guide the progress of the County technology year over year. CTA shall actively participate in all IT projects to ensure that they improve the capability and maturity of the Services.

The CTA provides the bridge between the deeply technical domain architects, business analysts and solution architects and other subject matter experts to ensure that the technology infrastructure meets enterprise goals, such as adaptability and complexity reduction. CTA shall work closely with Business Analyst Services to capture new or updated County business requirements as they are developed.

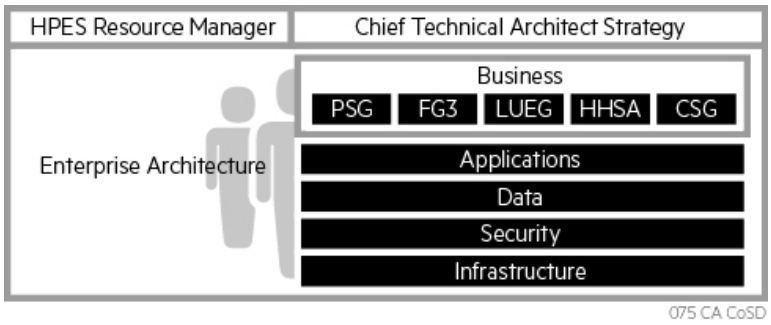
The CTA, together with the Enterprise Application Architect (EAA) and CISO, shall work directly with the CTO in the development and execution of architectural direction and strategy, develop and plan enterprise initiatives, identify and track emerging trends and changes to improve overall delivered Services, anticipate and understand transformative shifts in technology, develop and maintain enterprise and departmental roadmaps, ability to access leveraged resource subject matter experts, maintain strong relationships with leading technology partners.

The CTA shall work directly with CTO to review all requirements documentation and designs, establishing and maintaining IT standards (e.g. Bricks), patterns, IT guiding principles, and communicating decisions to all IT staff.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The CTA and the Architects are two major components of our technology team. The CTA will have overall responsibility for setting Architectural direction and strategy (work directly with the EAA, the CISO and CTO) identifying emerging trends, anticipating and understanding transformative shifts in technology, developing enterprise and departmental roadmaps, and maintaining strong relationships with our leading technology partners. The CTA shall develop, deliver, for CTO approval, all technology standards, guiding principles, patterns and design guidelines and criteria. The CTA shall continuously maintain them. The CTA will then translate this information and direction to the Architects for execution.

Figure 32. HPES' Architecture Team Assigned to the County



With its in-depth knowledge and understanding of the County, this team will help the County implement new technology to streamline services to its constituents.

The Architects, who will receive strategy and direction from the CTA, will be responsible for executing that strategy including adherence to methodologies, standard processes, best practices, accelerators, and standards.

While there will be a strong dotted-line relationship between the CTA and the Architects, the CTA will report to the Account Executive, and the Architects will report to the Technology Office. The intent of this structure is to unencumber the CTA from the administrative burden required when one has direct reports, including HR activities and staff professional development—these activities will be the responsibility of the Tech Office.

HPES believes this structure allows the CTA to focus on strategic direction and transformation to always look forward.

The CTA/Architect reporting structure mirrors that of CISO/Security Ops. The CISO has overall responsibility for all aspects of security (with the County CISO) while Security Ops is responsible for execution of those strategies as well as day-to-day activities (prioritization of tasks, allocation of resources) and HR administration.

The HPES architecture team is aligned to County organizations, as shown in Figure 16Error! Reference source not found., and they support each vertical business unit across the architecture layers. Our chief technical architect (CTA) assigned to support the County will provide strategic oversight and direction to the HPES architecture team. During the past 5 years, our CTA has fully immersed himself in learning and understanding the County's architectures, processes, and technologies. He is currently working with the County CTO to develop and maintain an aspirational technology roadmap for the enterprise. We will continue to build this relationship to further support architecture services under the new Contract.

The architecture team supporting the County has access to more than 9,000 HPES and AT&T architecture subject matter experts (SMEs). We established our architecture professional community with a common governance, including architecture job classifications to facilitate consistency of the EA architecture practice across HPES. The architecture profession at HPES is managed centrally and includes the use of an HPES Global Review Board to review and promote architects through their profession.

The combination of a top-down and bottom-up approach enables HPES to have a very flexible, driven, high quality and professional architecture program that can operate both vertically (architects with industry expertise) and horizontally (architects and subcontractor SMEs with technology expertise and focus) based on individuals skills and County needs.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES adheres to proven methodologies and processes across the organization that we adapted to meet the County's requirements. Our Architecture Services Methodology is based on principles that the County's CTO has adopted—principles precede requirements and they help frame the overall solution approach to align with County strategic direction.

In collaboration with the County CTO office, we reorganized the contents of architecture-developed Solution Design Documents (SDDs), summarized in Table 21, to align with our proven architectural methods (RightStep and ITSA) and holistic focus that encompasses business, data, applications, infrastructure, network, security, management and implementation aspects including solution evolution. This process improvement helped the County to obtain an architectural level of consistency regardless of who created the SDD. This customized template helps HPES facilitate consistent, completeness, coherency for all projects throughout the County.

Table 21. Solution Design Documents

SECTION TITLE	CONTENTS
Executive Summary	<Write a brief introduction describing the focus of this design document including, if applicable, the purpose, background and scope that affect the design of the project. This summary should be written in nontechnical terms as an introduction to the technical sections. It should contain enough information for a reader to get familiarized with what is discussed in the full document.>
Client Opportunity	[Use this section to describe client opportunities, problems, business drivers and/or goals. Include quotes or comments from clients if appropriate. Where appropriate, personalize the document for the client, mentioning the customer name and specific topics related to their environment.]
Proposed Design	<This section describes the logical and physical solution design including the physical architecture. Include one or more diagrams of the design either as an embedded picture or in the appendix. It is important to highlight that this template just provides guidance which must be tailored by the architect or engineer for their specific work. Not all sections and subsections are applicable to all solutions, and there may be some key ones missing for the solution you are designing. This is a template to help jumpstart the work at hand and provide ideas for design content that otherwise might be left out.>
Business Architecture	The business architecture defines the manner in which business strategy/mission, vision, governance, organization and key business processes come together to define

SECTION TITLE	CONTENTS
	the activities that deliver on the business strategy. Business architecture can be developed with a scope that encompasses an enterprise or solution scale. <This section is used if the impact to business from the implementation of this solution needs to be understood by the client stakeholders. For example, if there are significant changes to the way the client does business {business processes, roles of the client employees, business organization, etc.) here you would describe the logical changes to the business architecture. Each section would include the current and proposed architecture. <Template Sections 4.1.1 can be combined or split in two to describe the current and proposed business architecture>.
Data Architecture	< Data architecture provides a blueprint for the structure of the information components in the context of the business processes and the business organization, the application systems and their interactions (integrations), as well as the relationships between them. This includes the data, data service interfaces, and data management components and can be developed with a scope that encompasses an enterprise, solution or technology scale. <Template Sections 4.2.1 can be combined or split in two to describe the current and proposed Data Architecture>.
Applications Architecture	< Application architecture is the blueprint for the individual application systems to be deployed, their interactions (integration) and their relationships to core business processes of the organization. Application architecture can be developed with a scope that network requirements or touch points. <Template Sections 4.3.1 can be combined or split in two to describe the enterprise, solution, or technology scale, current and proposed application architecture>.
Infrastructure Architecture	Infrastructure architecture describes the software and hardware that effectively enables the deployment of other architectures. This includes IT infrastructure like servers, storage, backup devices, end-user devices, middleware, processing and standards used in operations, and does not include the network or communication components which have their own section. Infrastructure architecture can be developed with a scope that encompasses an enterprise, solution or technology scale. <Template Sections 4.4.1 can be combined or split in two to describe the current and proposed infrastructure architecture>.
Network Architecture	Network architecture describes the software and hardware that effectively enables the connection between infrastructure components and architectures. This includes networks, firewalls, load balancers, WAN, LAN, VLAN, communication devices and appliances, infrastructure device placement within the network, and the associated network standards used in operations. Network architecture can be developed with a scope that encompasses an enterprise, solution, or technology scale. <Template Sections 4.5.1 can be combined or split in two to describe the current and proposed Network Architecture>.
Security Architecture	< Security architecture is the blueprint for the structure of the security components of the overall solution, and how they are maintained in line with the security policies, both principles and requirements. It provides the central definition of the capability independent threat and vulnerability structure as well as disaster recovery. A security architecture can be developed with a scope that encompasses an enterprise, solution or technology scale.

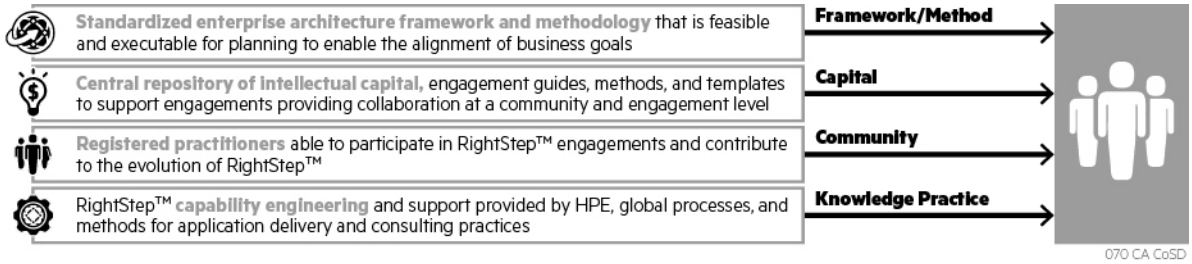
SECTION TITLE	CONTENTS
	<Template Sections 4.6.1 can be combined or split in two to describe the current and proposed security architecture>.
Acceptance Criteria	<Describe the success criteria and acceptance requirements guidance. This is at high level, acceptance test plans are created later in the lifecycle guided by these criteria but with much greater detail. This is to provide guidance to the architecture and design on how successful outcome will be measured by the stakeholders/client. business acceptance criteria would be those measured in terms of business goals, drivers, metrics, outcomes or results, if any ("Improve claim handling productivity by XX%">. Functional acceptance criteria by those that measure what is included (if the many areas of scope were included, functionality of given modules or components, non-functional requirements or qualities). Technical acceptance criteria are related to "how" the solution is put together (how the layers are put together {three tier architecture for example}, how the interfaces work, how the roles are spread across the many environments, etc.). Implementation acceptance criteria revolve around "with what" and in what order the solution is made {for example, database was required to be on Oracle, middleware and ESB using TIBCO, small project implemented first and later phased to full production, support personnel training, documentation standards and content, etc.}.
Implementation Considerations	<Describe the items that were addressed during the design phase of the project for implementation.>
Deployment	<Describe the technical details of the solution's deployment. Include architecture diagrams.>
Infrastructure Management	<Describe how the infrastructure is to be managed, operated and which companies or organizations will be responsible.>
Maintenance Plan	<Provide an explanation of the ongoing maintenance support model. Include reference to any existing agreements as well as any new procedures, processes or resource units.>
Evolution	<Describe the evolution requirements or special considerations that affect project planning and solution implementation aspects—order of implementation of the many components, changes in solution scale /size during the various implementation phases, bringing in highly specialized or hard to find resources, etc. This is not a repeat of other sections of the solutions, this is an extract of what project managers should watch for and take into account in the implementation, testing and development planning.>

Processes: HPES has two primary architecture methods recognized by The Open Group (HPES RightStep and ITSA). We also use other methods or frameworks if desired by the client. Most important is the architectural heuristics, as each method is designed to address a specific challenge. We use these with many clients as the starting point for setting the architecture standards and adapt our approach and work products to align to the client's needs. We assess each client situation to determine business need, maturity, and existing standards.

HPES developed and uses an IT transformation planning framework and methodology to create enterprise and business architectures. Known as HPES RightStep, shown in Figure 33 it is mapped to multiple benchmark and industry enterprise architecture frameworks, including GEAF, Zachman, Meta Group, C4ISR and DoD, Federal Enterprise Architecture Framework, and TOGAF. We map our architecture tools and processes to a specific framework when required by the client. For example, using RightStep we

can create a TOGAF compliant enterprise or business architecture. RightStep has been in place for more than 20 years at HPES.

Figure 33. RightStep Transformation Planning Framework



This flexible framework enables HPES to map our architecture tools and processes to a client-specific framework.

RightStep and ITSA align with the HPES framework and governance for consulting services, to facilitate integration with all other supporting methods and disciplines—grouped under the umbrella of the HPES transformation framework. This framework aligns and integrates the architecture with other HPES capabilities and methods that are necessary for successful transformation including business consulting, value management, management of change, program and project management, portfolio management, IT service management, SOA services, and governance.

- Automated Tools – Automated systems and tools involved in proposed solution.

To create architectural designs we use modeling tools such as EA Sparx, ProVision, and/or MEGA (MEGA is used on the Proctor & Gamble account by HPES) to represent business processes, models, and patterns that define the business architecture. To address IT transformation challenges, the HPES architecture team currently supporting the County will introduce HPES Enterprise Maps v3.0 MEGA as the business intelligence tool to provide comprehensive visibility across business functions, application components, servers, networks, system software, and financials using imports from PPM and County AppsManager. Using EA life cycle processes (for example, BRICK) and principles, Enterprise Maps MEGA enables comprehensive enterprise portfolio management to identify core systems, systems of differentiation, and systems of innovation to facilitate alignment with County business strategies.

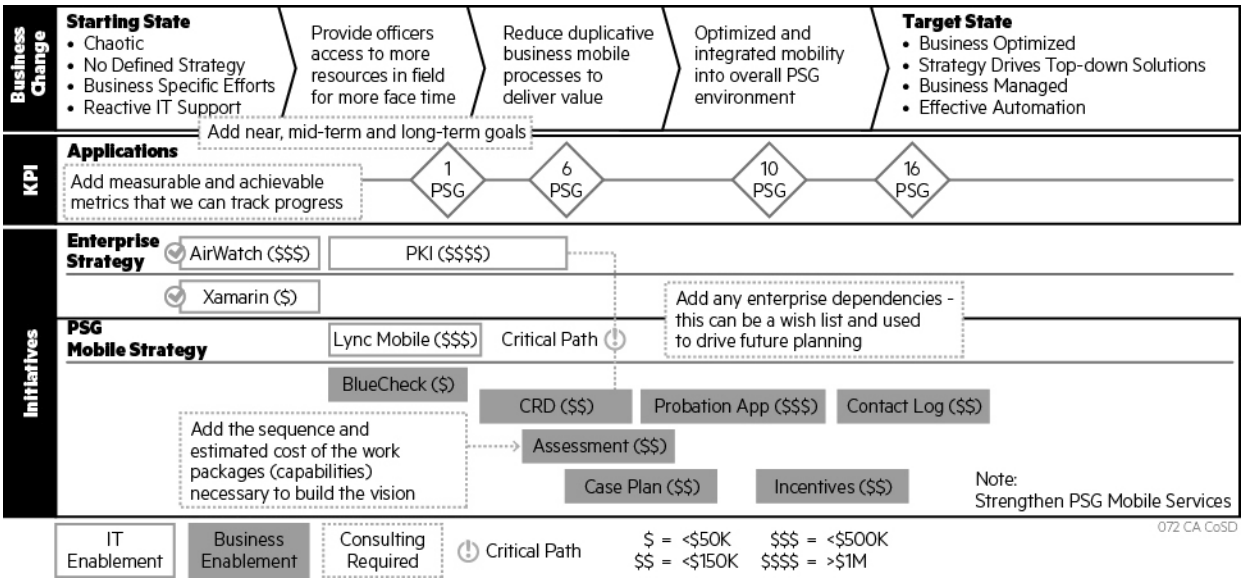
Tools, methodologies, and accelerators are used together, as detailed in Section 2.5.6.1, from HPES' Enabling Delivery and Global Excellence (EDGE) Platform Architecture Suite standards.

- Qualifications and Experience – Background and experience in comparable environments

HPES support of the County spans the past 10 years and has evolved as the environment changes to meet the demands of County employees and constituents for online services.

HPES created the sample Business Architecture Capability Roadmap for the County, shown in Figure 34 to illustrate which capabilities are enabled by which projects, KPIs, and investment factors. This is an example of a business value-driven approach that we use at the start of each potential project that comes out of the EA effort.

Figure 34 PSG Mobility Roadmap for the County of San Diego



This roadmap has facilitated many business management investment decisions.

As a pioneer in EA, HPES has provided decades of experience to our clients as evidenced by the following achievements:

- The first commercial consulting methodology to create principle-based architectures (1988).
- The first commercial architecture consulting methodology to use the 1986 Partnership for Research on Information Systems (PRISM) framework, the first known EA framework, which predates the Zachman framework. PRISM was the first in defining and initiating the use of architectural principles.
- To date, the only architecture methodology to create a continuous link across all the architectural principles up to the business drivers that motivated them
- Our architecture methodology has improved and evolved during 30+ years, predating TOGAF by 7 years.

HPES' qualifications and expertise are further demonstrated through our leadership and active contribution to numerous architecture standards bodies and groups, especially at The Open Group, where HPES is a Platinum member. Some additional examples of our leadership roles include:

- Board of Directors: The HPES Director of Standards has served 11 terms as Chairman of the Board of The Open Group and only recently a new chair has been appointed
- Business Forum: Leadership in the definition, development, and evolution of the standards generated from this forum.
  - An HPES SME was the initiator and chair of Board Workgroup Business Architecture Standard. HPES continues to significantly contribute to the standards emanating from this forum.
  - Participant of Business Forum as thought leader and HPES delegate at Board Workgroup Business Forum, 2009–2011.
  - Co-author of edicts from the Business Forum, accepted and presented to the IEEE conference in Luxembourg, "The Business Architecture Profession" September 2011
  - Co-chair of the TMF–TOGAF Workgroup and liaison, 2009–2013, W114
  - Leadership in the workgroup for IT governance, January 2010, W193

- Security Forum – An HPES SME chairs this forum, leading the definition, development, and evolution of security standards, for example the Cybersecurity Working Group that is developing standards for areas such as the Internet of Things.
- Healthcare Forum – An HPES Fellow chairs this forum. With his leadership this forum works on standards for the Federal Health Information Model and how to extend it globally
- Architecture Forum:
  - TOGAF Working Group – Evolution of the TOGAF ADM and frameworks next version
  - Open Certified Architect Working Group – Definition of the standards for this premiere professional certification; HPES SME chairs this working group. Both the chair and another HPES SME are listed as significant contributors to most standards from this working group.
  - Business Architecture Working Group – Developing the standards for the BA360 standard and its insertion into TOGAF.
  - ArchiMate Forum – Definition and evolution of this standard
- IT4IT Forum – An HPES SME chairs this forum for defining these standards
- Service Oriented Architecture Forum – Leadership in the definition, development, and evolution of SOCCI, Open Platform 3.0, and other SOA standards
- Real-time and Embedded Systems Forum – Leadership in the definition, development, and evolution of standards for the dependability and security of these systems,
- HPES participates in practically all other Open Group forums.

HPES is also a leading member of the ISO/IEC/IEEE Working Group on Architecture (JTC 1/SC 7 WG 42) where we significantly contribute to the projects on architecture frameworks and architecture description standards, as well as other areas.

Leadership in these governing bodies enables HPES to contribute to the architecture profession by l innovative and pioneering ideas for the practice. Our active participation enables HPES to stay in the forefront of architecture-related standards.

Table 22lists representative engagements involving EA services.

Table 22 EA Services Implementations

CLIENT	SECTOR	COUNTRY	SCALE
County of San Diego	Government	USA	Municipal
City of Anaheim	Government	USA	Municipal
City of LA	Government	USA	Municipal
Syngenta	Agricultural	Switzerland	Global
Telefonica de Bogota	Communications	Colombia	Country
Vodafone	Communications	UK	Regional
Grupo Bimbo	Consumer – food	Mexico	Country
CenterPoint Energy	Energy	USA	Country
Banco de Credito e Inversiones	Financial Services	Chile	Country
Banelco	Financial Services	Argentina	Regional
Flemish Government	Government	Belgium	Municipal
Oregon Secretary of State	Government	USA	Municipal

CLIENT	SECTOR	COUNTRY	SCALE
Conservation International	Government – NGO	USA	Global
GM	Manufacturing	USA	Global
Spirit Aero	Manufacturing	USA	Country
Nissan North America	Manufacturing	USA	Regional
Vaillant Group	Manufacturing	Germany	Regional
US Airways	Transportation	USA	Country

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None at this time.

2.5.6.1. Describe your proposed approach to Application Architecture, including processes and artifacts that will help the County identify and address linkages and dependencies with infrastructure changes.

HPES takes a holistic approach to application architecture that recognizes the linkages and dependencies associated with infrastructure changes. Within HPES, we define solution architecture as "the essential, unifying concept of an information system and its effective deployment into an operational environment to solve a key business problem." Solution architectures are more project or program related architectures and include all architectural domains and subdomains for the given solution including business, application, data and technology, information, security, and infrastructure architectures. Thus an application architecture is viewed as a component of a Solution Architecture, and at the County, Solution Architectures are detailed in the SDD, described in the Methodology and Key Processes section above. Our applications architecture will include application principles, integration models, application landscape models, application portfolio maps, application to process maps, application flow models, application to information matrix, and application standards, among others. These will be organized within topic areas (sometimes called domains and subdomains) and supported by RightStep, as described above.

2.5.6.2. Describe your approach to staffing and organization of Architecture Services.

HPES' global architecture capability is an organization with a formal charter and governance model within ES that supports all aspects of architecture services—methodologies, processes, best practices, accelerators, standards, and professional development. This applies to all architects, whether enterprise, solution, business, or technology architects. This is consistent with our approach to create architectures that seamlessly provide guidance from the enterprise scope to the solution and technological layers. The guidance and standards provided by the ES architecture capability team is also used by other business units. Architecture capabilities/teams reside throughout HPES, in both accounts and in local and regionally available teams that can be leveraged as an element of a client engagement. To facilitate the organization of architecture services, a collective set of standards, best practices, tools, and accelerators for each strategic capability are kept within the HPES EDGE platform.

2.5.6.3. Describe your proposed approach to a common architecture toolset and documentation standards, including benefits to the County.

HPES's approach to a common architecture and tool set is described above in the Automated Tools section. Additionally, our architects regularly conduct whiteboard sessions with other team members—security, application, the County, and other vendors—before we create an SDD for any project. The

updated SDD template, included in the Solution Summary and Rationale section above, covers all necessary architecture artifacts and design consideration, which includes high availability, scalability, County architecture/network patterns, reuse of existing County technology assets, leading to complete, consistent and coherent solutions. HPES also uses this document for internal reviews as the standard template for architecture projects from start to finish. Every SDD document is also used in its entirety in downstream activities, for example, by engineers for technical design documents, run books, server builds, load balance workbooks, and firewall changes. This approach facilitates consistency across all projects from design through implementation.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Enterprise Application Architect (Schedule 4.3, Section 2.23)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES' architecture approach defines a continuum both from top-to-bottom (strategy to technology) and end-to-end (advise to manage), where architecture is integral to every County strategic initiative – not just a standalone practice. During the past 5 years, HPES has played an integral role in advancing architecture practices and governance with the County. We have an in-depth knowledge of how enterprise architecture (EA) services function and their impact on the County's mission and consider these services as a key enabler and driver to move the County forward.

> Gartner observes that HPES' Enterprise Architecture program is the "foundation of Transformation planning. It (HPES EA) views EA as a business-enabling continuum—from top-level business architecture (BA), through the different viewpoints of EA (for example, IA, SA and TA), and down to the programs, projects, and initiatives that enable targeted business outcomes."
>
> *Gartner Magic Quadrant for Enterprise Architecture Consultancies*

Rationale: HPES sees the Enterprise Application Architect (EAA) as a key role in the architecture continuum, specifically being responsible and accountable for the "advise to manage" (illustrated in Figure 35) portion of the enterprise architecture, while supporting the CTA, CISO and CTO in the "strategy to technology" portion. The EAA shall work directly with CTA and CTO to review business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, align with information management strategies and overall efforts to continuously improve the provision of Services. The EAA shall manage and promote the use of County standards, related to software applications, promote the reusability of existing services and expanded use of County platforms, serve as a subject matter expert to projects and provide support for IT project teams. The EAA provides the bridge between County business and the IT staff that ensures that the application architecture meets business goals and objectives, that promotes reusability and provides data and interface connectivity across the Enterprise.

Figure 35 HPES' EA Methodology

Our straightforward methodology, based on recognized and proven Open Group practices (HPES RightStep, IT Solution Architecture [ITSA] and The Open Group Architecture Framework [TOGAF]) to engage with the County on these fundamental enterprise and business architecture issues.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The CTA and the EAA are two major components of the HPES architecture team. The EAA shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements and act as a subject matter expert on the effective use of technology in developing County business solutions. Working with the CTA, CTO and CISO, once overall architectural strategy and direction has been established, the EAA shall advise IT staff regarding the feasibility of their proposed approaches to project solutions in terms of systems capabilities, new technologies and alignment with established application architecture guidelines and standards. The EAA has overall responsibility for IT strategy execution across the enterprise including adherence to methodologies, standard processes, reference IT patterns, accelerators, and standards.

.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES adheres to proven methodologies and processes (RightStep and ITSA) across the organization that we adapted to meet the County's requirements. Our Architecture Services Methodology is based on principles that the County's CTO has adopted—principles precede requirements and they help frame the overall solution approach to align with County strategic direction.

Processes: HPES has two primary architecture methods recognized by The Open Group (HPES RightStep and ITSA). Since the EAA is focused on solution development across the lifecycle, the EAA will be primarily using HPES' Global Method of IT Strategy and Architecture (ITSA). ITSA is HPES' methodology for developing solution, initiative, or technology architectures. It is a structured as a participatory approach that involves key stakeholders in the client's business. It has been proven effective through many years' experience in defining, guiding, and evolving complex information systems in multiple application domains. ITSA helps architects understand the needs of all stakeholders by viewing the architecture from four vantage points or views:

- Business View – *Why* is the engagement being done? What are the motivations and business drivers?
- Functional View – *What* will the system do? What information will it provide?
- Technical View – *How* will the system be realized with IT components?
- Implementation View – *With what* specific products and other components will the system be implemented? In what organization? According to what plan?

ITSA defines each view using principles, models, and standards appropriate for the business domain. When combined, the four views enable HPES to understand the needs of all stakeholders and create a snapshot of the solution. Business factors (drivers, goals, metrics, principles, models, and standards) are the basis for all technical and implementation decisions. The methodology does not specify (or limit) the techniques to use to gather the business information or products to solve the customer's problems and compliments each client situation to determine business need, maturity, and existing standards.

- Automated Tools – Automated systems and tools involved in proposed solution.

To create architectural designs we use modeling tools such as EA Sparx, ProVision, and/or MEGA (MEGA is used on the Proctor & Gamble account by HPES) to represent business processes, models, and patterns that define the business architecture. To address IT transformation challenges, the HPES

architecture team currently supporting the County will introduce HPES Enterprise Maps v3.0 MEGA as the business intelligence tool to provide comprehensive visibility across business functions, application components, servers, networks, system software, and financials using imports from PPM and County AppsManager. Using EA life cycle processes (for example, BRICK) and principles, Enterprise Maps MEGA enables comprehensive enterprise portfolio management to identify core systems, systems of differentiation, and systems of innovation to facilitate alignment with County business strategies.

Tools, methodologies, and accelerators are used together, as detailed in Section 2.5.6.1, from HPES' Enabling Delivery and Global Excellence (EDGE) Platform Architecture Suite standards.

- Qualifications and Experience – Background and experience in comparable environments

Refer to section 2.5.20 for HPES County qualifications over last 10 years, industry recognition since 1988, and reference accounts.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None at this time.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Innovation Management Services (Sched 4.3, Section 2.24)

Innovation Management Services will support the transformation and innovation model of continuous progressive change in how Services are delivered. This includes, but is not limited to, delivering Services via a bimodal approach, with an emphasis on exploration, agility, and speed, while still maintaining operational integrity and stability.

Innovation Management Services will begin at CED with presentation of a qualified Innovation Officer (IO) to the County for County approval. The IO shall develop for County approval a program charter and rules of engagement that will define the process to:

- identify potential needs/issues/gaps/opportunities for improvement
- create a list of potential services available to further innovation and transformation, to include:
  - joint development workshops
  - white-board sessions
  - prototypes
  - pilots
  - demonstrations of products, software or services
- design and develop lab environment(s) and rules of use
- determine method to define success criteria
- define collaborative engagement model with EA, CTA, EAA, CISOs and County Business Leaders

Innovation Management Services shall include an Innovation Management Office that will serve as the foundation for continuous business improvement, innovation, and transformation. The Innovation Office (IO), established and staffed in January of CY2, shall be a cross-functional team with the directive to drive IT innovation/transformation and create a true environment of agility and high-velocity change at the County.

IO shall work with County CTO and County Business leaders to identify specific actions in support of County Excellence Goals. This will result in a series of initiatives in which Contractor shall propose solutions, business case analyses, anticipated pricing, and project timelines and resource plans. The proposed initiatives will be reviewed by the Innovation Management Review Board and, if approved, shall be executed using (as appropriate) agile and rapid-prototyping methodologies.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The Innovation Officer will be based at HPES' Rancho Bernardo facility. The Innovation Management Office will be a virtual office with some members residing at HPES' Rancho Bernardo facility and others at US-based facilities as determined by skillset required.

Starting with CY2, Contractor recommends an Innovation Core Team of three (3) persistent members:

- Senior Technologist (skillset akin to CTA)
- Senior Solution Architect
- Senior Business Analyst

Addition personnel will ebb and flow through the Team as required by Innovation/Transformation ideas/pursuits/opportunities.

Additional personnel could come from the County, Contractor, Contractor's partners or other 3rd parties and could include:

- Business Leaders
- Senior Technologists
- Innovation Lab Personnel
- Local Government advisory personnel (e.g.: Gartner)
- Architects/Engineers
- Business Analysts
- Software Specialists
- Logistics Engineers
- Mobility Specialists
- Change agents
- Logistics experts
- Asset and Billing Specialists
- Government Strategists

At execution, Contractor will propose utilization of an existing RU aligned with the skillset of the team member. If an existing RU cannot be utilized for the activity to be performed, Contractor will propose an hourly rate or FFP for County consideration. Rates will be agreed upon in writing by the Parties.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Methodologies and key processes shall be defined by the charter and rules of engagement.

Governance will be provided by the Innovation Management Review Board, co-chaired by County CIO and Contractor AE who will have joint approval on all proposed initiatives and activities.

Contractor shall perform an annual assessment of Innovation management Services for County review and approval. Contractor suggests adding this report to Schedule 5.

- Automated Tools – Automated systems and tools involved in proposed solution

CY1: none. CY2 and beyond: to be determined by Innovation Management Services charter and deliverables.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

2.5.15 Executive Summary

The Cross Functional Services Framework provides essential program oversight to make sure the County's IT environment is effectively managed, end-to-end, and with full and open transparency.

As is being accomplished today, The HPES cross functional services framework will implement industry best practices process, quality, and project methodologies to align processes to people and technology to fulfill the County's mission and vision.

This centrally managed cross functional framework will also serve as the primary focal point between County IT management and the individual services frameworks on matters relating to operational issues. The County will be able to interface with a single focal point rather than having to locate the right person within individual services frameworks.

The goal of the architecture for cross functional services is to provide services that consider a holistic or end-to-end enterprise view across all IT frameworks. Built on a uniform platform and methodologically driven, the framework provides for improvement in the efficiency and effectiveness of the services delivered to the County through the use of common repositories and time sensitive updates to information and establishment of prescribed interfaces.

Cross Framework Component Integration Components

As described in previous sections, our approach is to leverage and build upon the County's existing systems, resources and processes. Our solution will now wrap a County service portal around the applications and reports to provide the County with a common entry point and consistent look and feel.

The System and processes that currently exist in the County will remain in place upon contract award. These include:

Contract and Acquisition Management Services

The HPES solution and approach will include an experienced, full-time contracts manager to serve as the single point of contact for the County on all contractual matters, including subcontracts and third-party vendor relationships. Responsibilities will encompass all contractual issues between HPES and the County, including contract interpretation, work requests, estimates and pricing discussions, and contract changes and disputes. HPES believes that contract management is an ongoing process that makes certain the County receives the expected IT and telecommunications services.

The contracts manager will establish contractor oversight responsibility and provide recurring status reports to the County contracts manager on contractual matters and will work with County stakeholders to respond to unscheduled requests for information. In addition, the contracts manager will interact with subcontractors and vendors to audit and verify the timely provision of the requested services. The keys to successful contract management are an unambiguous and mutual understanding of the contract and a good business relationship. The performance standards must be articulated in the contract so that HPES and the County completely understand the standards and process for meeting each standard.

Integrated Asset Management Services

HPES will provide an Integrated Asset Management System (IAMS) that reduces the amount of manual intervention required to verify, check, and fulfill requests while adhering to governing policies and standards.

It is important that we answer five fundamental questions to demonstrate the scope and dimensions of effective asset management:

- What do you have?
- Where is it?
- How well is it working?
- How much does it cost?
- How well does it support your business?

IT asset management (ITAM) will address these questions by providing processes, tools, data, and people across the entire life cycle. Risks associated with IT assets will be articulated and managed because ITAM manages the legal obligations associated with vendor warranties and support commitments, entitlements, and asset disposal.

Our solution is based on an upgrade to HPES' Asset Manager from Asset Center. Asset Manager influences IT operations and decision making in the following ways:

- Aligns services to their supporting assets and contracts
- Effectively manages contracts, leases, license agreements, and warranties
- Streamlines the fulfillment of goods and service requests from the service catalog
- Effects complete asset and project audit tracking
- Proactively identifies license compliance issues
- Evaluates opportunities on license maintenance
- Re-harvests and reallocates unused software licenses

HPES Asset Manager HPES currently uses Asset Center, which will be upgraded to the enhanced HPES' Asset Manager prior to the start of the new contract. This upgrade will be performed as part of the current contract and will be seamless to the County and its users while providing enhanced performance.

Billing Management Services

We designed the current billing management systems and processes to provide accurate and timely invoices with an appropriate level of detail; generate electronic billing information to facilitate the County's chargeback activities; and support activities required to audit, validate, and substantiate billing.

The methodology and processes used comprise a combination of standard billing methodologies developed by HPES across our client accounts as well as those developed in conjunction and in compliance with the County billing and management policies. Our methodology includes performance-based management as well as periodic assessments of HPES' Key Performance Indicators (KPIs). As an integral component of our quality assurance program, we continually assess these KPIs to identify

negative trends. We conduct root-cause analyses where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, facilitating year-over-year continuous improvement.

We use the following tools to manage Billing Services:

- IBilling – HPES' billing data consolidation application based on SQL Server and SQL Server Integration Services (SSIS).
- iTrack – The County's customized implementation of Nicus' M-PWR commercial off-the-shelf (COTS) chargeback application
- Billing Source Data Tools –
  - AssetManager
  - ServiceManager
  - PPMC
  - Active Directory
  - myRequests (myRequests will be replaced with Service Catalog and Request Manager during the Cross Functional Transition as described in Section 2.11 Transition Services Framework, 2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5), Special Cross Functional Project – Replacement of myRequests)
  - AppsManager
  - CSRFs
  - Work Requests and ISRs

Security Management Services

The NIST based RMF fundamental tenets of security include controls that are specifically designed to protect confidentiality and Integrity of data. At a high level, the controls include the creation of policies and procedures, awareness and training, conducting Privacy Impact Assessments (PIA), identifying and classifying sensitive information, and record retention and disposal of information. Some other control specifics are described as follows:

- **Access Enforcement** – The County controls access to confidential data through access control policies and access enforcement mechanisms. At the enterprise level, employees are part of role based Active Directory groups that is determined via a Change Security Request Form with approval and consent of a direct employee supervisor. Other non-enterprise systems control access with local management capabilities. As part of the roadmap, a full enterprise identity management capability will be in place to better secure and manage access controls.
- **Least Privilege** – HPES enforces the most restrictive set of rights and privileges for each user in a specific role. Concerning confidential information, HPES make sure that users that must access this information only have access to the minimum about of data that are necessary to perform their job duties.
- **Auditable Events** – HPES monitor events of systems that have confidential information. There are regular reviews and analysis of system records that indicate inappropriate or unusual activity affecting confidential information. Investigations occur when suspicious activity is detected and violations are reported.
- **Identification and Authentication** – County users can be uniquely identified and authenticated before accessing confidential information.
- **Media Access** – HPES restricts access to media containing confidential information, often through encryption. Media includes CDs, USB flash drives, backup tapes as well as non-digital media such as paper.

- **Media Transport** – HPES protects digital and non-digital media including confidential data transported outside the organization. There is a data transfer request process to scrutinize the data (often encrypted) that leaves County premises.

All of these sets of controls are implemented at the infrastructure level and on applications that process confidential information. The visibility over how effective controls are being on the lookout for new threats, identifying vulnerabilities, and having a sound mitigation strategy to eliminate or minimize risk result in an optimally protected enterprise.

Service Delivery Management (SDM) Services

While ITIL certified processes and collaboration will be the foundation for our processes and approach, the key element is assigning a single service delivery manager (SDM) to act as a point person for each business group. This service had been provided to the County previously and was proven to be very valuable to the account and to the customer, giving each business group a single point of contact to reach out for assistance with any of their business needs and requirements. SDMs will perform most of the duties the incident managers do today in the current model and will include the following at a minimum:

- Incident management
- Problem management
- Change management
- Release management
- Escalation management/Service Request status
- Communication
- Billing management
- Availability and capacity management
- On-call rotation

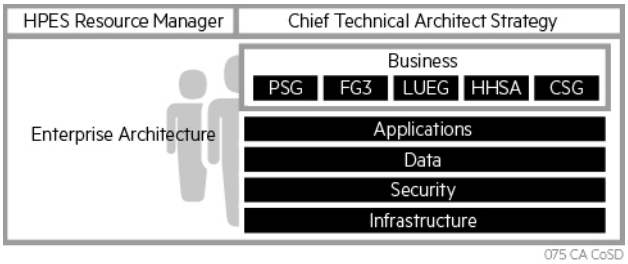
The on-call rotation in which the SDMs participate is critical to facilitate centralized after-hours support to the County for issue resolution as well as making sure each SDM has appropriate amounts of time off and vacation as required. HPES is proposing five SDMs who will rotate on-call every five weeks. During business hours (Monday through Friday 6:00 a.m. to 6:00 p.m.), each SDM is responsible for their own business group. After hours and on weekends, the on-call SDM takes primary responsibility for any issue and works it to resolution. If an enterprise issue emerges during business hours, the on-call SDM takes point for this issue initially—and possibly to completion, depending on the scope of the issue. If an issue arises during this time within the business group for that on-call SDM that requires their focus and attention, another SDM will be assigned to take over the new issue. All SDMs from each business group will be required to work any/all enterprise related issues/disasters that require a shift rotation. The on-call SDM will verify that the correct customer from the business group is notified and that the SDM assigned to that business group is aware if anything has occurred in their space so they can address it. Problem management is a day-to-day responsibility for the SDMs, and they will be assigned activities to work whether it be proactively or through tickets, escalations, and so forth. HPES has a primary owner—the enterprise problem manager—who will report, track, and communicate all problem management issues worked by the team and the account as required in the weekly CTO Operations meeting. Each SDM will also report any problems being worked by them through this process that impact their business group or the enterprise in the monthly portfolio review meetings that they will be required to attend.

Architecture Services

The HPES architecture team is aligned to County organizations, as shown in Figure 36, and they support each vertical business unit across the architecture layers. Our chief technical architect (CTA) assigned to support the County will provide strategic oversight and direction to the HPES architecture team. During the past 5 years, our CTA has fully immersed himself in learning and understanding the County's

architectures, processes, and technologies. He is currently working with the County CTO to develop and maintain an aspirational technology roadmap for the enterprise. We will continue to build this relationship to further support architecture services under the new Contract.

Figure 36. HPES' Architecture Team Assigned to the County



With its in-depth knowledge and understanding of the County, this team will help the County implement new technology to streamline services to its constituents.

The architecture team supporting the County has access to more than 9,000 HPES architecture subject matter experts (SMEs). We established our architecture professional community with a common governance, including architecture job classifications to facilitate consistency of the EA architecture practice across HPES. The architecture profession at HPES is managed centrally and includes the use of an HPES Global Review Board to review and promote architects through their profession.

The combination of a top-down and bottom-up approach enables HPES to have a very flexible, driven, high quality and professional architecture program that can operate both vertically (architects with industry expertise) and horizontally (architects with technology expertise and focus) based on individuals skills and County needs.

Project Management Services

The enterprise project management office (EPMO) and project management staff will be a centrally located at the HPES Rancho Bernardo facility. We will join the County at their facilities when necessary to drive successful communication at the program and project levels. This facility approach enables interaction between the project management staff and all Customer and HPES portfolio towers, including:

- County Technology Office (CTO)
- County Group IT Management (GITM)
- County Department IT Coordinators
- County Project Sponsors
- HPES Account and Operation Management
- HPES Applications Portfolio Management
- HPES Infrastructure Operations
- HPES Account Security
- HPES Technology Office
- HPES Business Management
- HPES Contracts Management

Using the aligned HPES/County organizational structure, we implement a formal communication procedures that engages internal and county stakeholders. Some examples of interactions include the following:

- Establishing communications strategies for the specific needs of the CTO and County business groups
- Developing enterprise communication procedures and templates
- Auditing program and project communications plans
- Creating EPMO announcements followed up by direct communication with impacted stakeholders
- Developing and maintaining communication vehicles such as the EPMO SharePoint,
- Creating and executing communication plans for EPMO initiatives
- Preparing presentation material for internal and external reporting.

In addition to communication at the program level, the HPES PMs, as governed by the HPES EPMO, interact with the County in a number of ways:

- Regularly meet with the project sponsors, County Group IT Managers (GITMs), and members of the County Technology Office (CTO) review status and to discuss project concerns, activities, risks, issues, or any needed escalations
- Support county sponsors with remediation efforts as necessary to verify County satisfaction with project performance
- Confirm we remediate and follow through on risk items to County satisfaction and successful project delivery
- Partner with sponsors and vendors to deliver a consistent and predictable customer experience.
- Maintain a list of project stakeholders, their role and contact information of all who are involved with the project. This list is distributed to all stakeholders.

Integration and Testing Services

Our approach to developing the testing strategy is to supplement and support the project life cycle with the following testing-specific information:

- Testing roles and responsibilities
- Testing methodology
- Test levels to be performed
- Test coverage to be performed for each test level
- Test deliverables
- Test management and measurement approach
- Required testing environments and tools.

Testing activities require planning and management to fully succeed. Based on the priorities identified in the test strategy, we develop a Test Plan that covers each required test level and provides tactical guidance by specifying the following factors:

- **Test Scope** – Scope of the HPES team's testing services to be provided, including test types
- **Test Schedule** – Schedule for all phases of testing, integrated with the overall project schedule (test development, test execution, testing metrics collection, and testing reporting)
- **Test Roles and Responsibilities** – Test roles/responsibilities for all participants, including the HPES team, State staff, and any third-party vendor staff; responsibility for test environments and tools
- **Test Design/Methodology** – Test case design techniques/strategy for each test level
- **Test Procedure/Execution** – Test-level execution tasks, including participants, to conduct execution; entry, exit, pass/fail, suspension, and resumption criteria for each test level

- **Test Tracking and Reporting** – Test results data collection requirements, documentation, and reporting; test progression tracking and error/deficiency management/resolution process; any risks specific to a test level that require mitigation.

The HPES Test Plan also outlines the recommended testing tools and testing management and measurement.

A critical part of the test plan is implementing testing management and measurement to make sure that testing meets the project requirements. We understand the best testing strategy and test plans can succeed only if well implemented. HPES applies and adapts the processes, techniques, and templates of our testing method to effectively manage and control the planning, execution, and completion of all testing activities. Testing management and measurement involves the following actions:

- Establishing and maintaining detailed estimates, a test schedule, resource plans, and procedures for all testing phases
- Managing preparation of test plans, scenarios, and test cases for each test level
- Establishing Acceptance Criteria
- Managing the execution of test cases, tracking and resolving defects, and verifying completion of tests, including regression testing when necessary
- Managing testing close-down, including reporting

Incident Management Services

HPES' primary integration for IM is HPE Service Manager Enterprise Suite, a comprehensive, fully integrated ITSM solution that leverages more than 25 years of service management focus and experience. It provides a powerful platform to standardize, automate, and enforce key IT processes and demonstrate value to our customers. It offers efficiencies through automation of core IT processes such as incident, problem, service level, and end-to-end change and configuration management. The suite orchestrates ITSM processes and enables customers to track calls, requests, incidents, problems, changes, releases, configurations, and SLAs. Our customers know who is responsible for every task, what has been done, work remaining, and whether the task is on schedule.

Problem Management Services

HPES will continue to enforce a standard "plan, do, measure, adjust" methodology to continuously recognize, react to, and correct problems quickly. Team members are trained to report all issues to the appropriate SDM or enterprise problem manager, who will identify the owner responsible for resolution. If the owner fails to resolve the issue within a specified time frame, the SDM will initiate our predefined escalation process to prioritize and broaden the focus on resolving the problem. Any individual, County, or HPES employee, may identify a problem although they usually originate as incidents or changes. As a standard practice, we conduct enterprise-level delivery reviews weekly to share experiences across the IT services and cross-functional frameworks to identify and mitigate risks. These efforts and practices have contributed to successful communication of the issues being worked as well as the resolution of issues. Relevant examples include Outlook disconnects, antivirus pushes, and site latency.

Change Management Services

The HPES IT Change Management Suite and Services supports multiple types of change requests and understands the risks associated with potential requests. Most importantly, it integrates change processes into the broader ecosystem in a cost effective way, providing full and open transparency and progress reporting. Our new Change Management Suite tool will assist in the continuous improvement needed in this framework, will greatly enhance configuration visibility and stability, as well as monitoring the type

and frequency of upgrades that may be required. While costs continue to be constrained with this HPES solution, the real benefit will be realized through increased stability and predictability.

HPES IT Change Management is part of an integrated set of ITSM process modules for Service Manager.

The HPES IT Change Management Suite comes with embedded, out-of-box IT Infrastructure Library (ITIL) based best practices. It creates mechanisms for measuring change process workflows, automates impact analysis, and enhances Change Request Control Board (CRCB) virtualization. The HPES IT Change Management Suite has been used to successfully implement numerous County change requests. The suite also improves collaboration and efficiency across the various roles such as the change coordinator approvers and managers. Additional efficiencies include minimization of total time to process changes, a feature supported by enabling the changing of approvers via smart phone. This feature facilitates approval of changes anytime, anywhere.

All changes will receive County approval through a formal change approval process as follows:

- When a change is desired the Change Initiator will complete a Request for Change (RFC) Ticket.
- The RFC is reviewed in the internal TAB review before released to the County stakeholders
- The RFC is submitted to the Change Release Control Board (CRCB). The CRCB consists of both HPES SMEs and County CTO representatives.
- The CRCB reviews the RFC and approves the change or disapproves it
- If the change is approved, the Change Initiator is notified as well as County End-Users and a Change Release is initiated.
- The Change Release is monitored through implementation and closure
- A PIR is completed for each change at the completion of the RFC

Release Management Services

The foundation of HPES' Release Management Services is our proven ITIL certified processes, of which release management is an integral component. While the enterprise release manager on the account is responsible for tracking and logging all releases, the Service Delivery Manager (SDM) per business group, will perform this critical role. The SDM will be responsible for understanding, monitoring, and assisting in the communication of these releases as they are completed in their respective business group.

In addition to the release review meeting that the release manager will hold with the HPES and County stakeholders, releases will be reported in the regularly scheduled meetings that the SDM will be required to attend that fall within the scope of their duties. The goal for each SDM is to understand all of the information related to the releases affecting their respective business group, bringing in SMEs if additional information is required.

Release management falls under the governance of the Change Release Control Board (CRCB) that consists of both HPES SMEs and County CTO representatives. All Configuration Items distributed into production use a formal Release Management process. HPES develops a Release Plan that outlines the release schedule, content of the release, and back out plans. Release Management works with Configuration Management to make sure the Definitive Software Library master IT configuration items remain current.

Configuration Management Services

HPES will provide a Configuration Management System (CMS) and multiple CMDBs, accessible through the Service Portal that supports activities associated with the recording, tracking, updating and disseminating the County's configurations for all assets, including network assets. The CMDB, integrated across the organization and service frameworks, will support all logical configurations of Hardware and Software supporting the Services, contain mappings to physical configuration, inventory data of

Hardware and Software, analyze trends and be used to manage and reduce Incidents and Problems. The Service Portal will show all of the information related to all assets from each tool mentioned above.

HPES will continue to provide Software Configuration Management (SCM) via Apps Manager for the County of San Diego portfolio applications and make sure version control history and that current versions of portfolio code and artifacts are available, including the application code, software tools, and artifacts. Application's SCM is part of the Program CM and conforms to those policies and procedures.

Discreet item identifiers will be associated with all Configuration Items (CIs). Applications' CIs include source code, compiled and/or linked code, packaged code, development environment tools and any related documentation such as user manuals, test scripts, test results, project management documentation, architectural drawings, run books and helpdesk scripts. HPES SCM will provide physical and logical on-line libraries for the configuration management of all software CIs.

HPES will provide hardware related information from ESL which is where datacenter related equipment is tracked and controlled and Asset Manager which includes the desktop related hardware items

HPES SCM will provide three libraries for applications code: two based on platform and one for vendor-delivered media. While Mainframe code will reside in the legacy Endeavor library on the mainframe, windows and midrange code will reside in the Team Foundation Server (TFS). TFS, more than a version control system, uses a SQL Server database as a means of scaling to large environments and infrastructures. TFS is key component in the life cycle platform, which will enable third-parties, customers, and solution providers to extend the base functionality with new features and customize the tool for the unique County requirements and initiatives.

HPES SCM will manage third-party vendor code to include contracted code, public domain, purchased and COTS packages. Third-party vendors will use TFS for development of all applications CIs, unless a program-approved provision is in place for off-site development for that application. The third-party vendors will make sure all code and artifacts are delivered as per contract. HPES SCM will review the third-party SCM practices and make sure the vendor deliverables are placed under configuration management for the program.

HPES and County-contracted third-party vendor code developed or maintained offsite will follow County security and HPES SCM standards. The County will be responsible for notifying their contracted third-party vendors of the requirement to follow security and SCM code control. Purchased, public domain, and COTS software packages will be implemented following County Security requirements.

Capacity Planning and Performance Management Services

Focused primarily on the capacity and technical performance of the hardware and software involved in IT Services, HPES capacity planning and performance analysts will collaborate with appropriate stakeholders in determining the resources required and ensuring performance or availability constraints will not adversely affect County business. Response times and quality of services for End-Users will be used as input and relevant data points to these decisions and performance assessments.

This section covers the process of Capacity Planning. The process goal is to make sure that IT capacity exists and is matched to the current and future identified needs of the County. The services in scope minimally include application and infrastructure servers, storage, desktops and network.

The primary input to this process is capacity planning information, sometimes called Performance Monitoring metrics in industry literature, such as UNIX and Windows performance information, or network performance information, from various tools. There are other monitoring tools for Mainframe, AS/400, storage, networks, etc. The secondary input to this process is inventory information, which helps the County and HPES to understand the context of the performance information, and to route it to the

appropriate County or HPES people. Examples include tools for the Data Center server inventory, the Applications inventory, the Billing list of low orgs and their corresponding County Business Units, etc.

The primary output of this process is hardware, software and configuration updates to the servers, storage, desktops and network to make sure the goal is met.

The process involves the assembly of accurate reports of shortfalls, analysis on those shortfalls, and development of a solution to solve any capacity items that do not meet the goal. The responsible framework may also need to obtain County funding approval. The solution is then implemented using existing Data Center procedures that may include County Change approval. Virtual server implementation requires re-configuration and can be done quickly, while implementation of physical servers may require the installation of new hardware, software and/or configuration items. Changes recommended and approved will be processed through the Change process for implementation. After implementation, the responsible framework verifies the effectiveness of the solution.

Development of Annual Capacity Management Procedures (ACP) is a key component of the HPES solution. The purpose of ACP is to forecast County IT capacity and performance requirements on an annual basis and reaching forward. The requirements definition, based upon historical performance, provides the basis for continuous improvement while ensuring Cost-Benefit-Analysis (CBA) confirmed County IT operations and service delivery. The ACP balances needs over the long term to optimize the resource workload expected in coming years. The primary inputs to the ACP process are historical performance information over the past year and the CTO technical roadmap to make sure the forecast encompasses all data needed to continue to meet the immediate and extended future capacities needed to meet all service levels.

The output from this process is the projections about the coming two year's IT capacity necessary to support the forecast, including identification of OS Upgrades required to support the forecasted capacity.

Because of the strategic significance and planning impact to service delivery for the future of the environment it is important to understand the basic assumptions underlying the plan. The following list identifies some these important assumptions regarding the ACP:

- Business forecasts are preferred over historical trends
- The annual capacity plan output identifies future issues needing solution, and provides many supporting details, but does not produce the solution itself.
- Holdovers from the previous year assumed to be addressed in the previous year. That is, current shortcomings are ignored.

The initiation of the ACP for report delivery to the County for review and approval begins during the mid-October timeframe to make sure a sufficient lead time for delivery of this annual report. The ACP report framework components for the County Program are overviewed in the following sections.

The Cross Functional Capacity & Performance Management process assembles the prior year's historical information, with inclusion of business forecasts, and produces the forecast over the planning period, including identifying OS upgrades if required.

The ACP is used to tune the Performance Management process for the new workload, and also to selectively identify problems/opportunities that should be undertaken as Projects to mitigate some of the workload. The Performance Management process collects current system capacity and/or performance data and performs predictive analysis to identify when the current capacity will exhaust. This data is stored and used in Annual Capacity Planning as historical information.

New desktop hardware technology is reviewed annually by Desktop engineering. Capacity and performance specifications for desktop hardware and desktop applications in use or planned are reviewed

with the vendors to accommodate current and future County requirements and expectations. A report of recommendations is presented and reviewed with the CTO. The information collected throughout the year is incorporated into the ACP to make sure adequate Desktop services to maintain service delivery.

Disaster Recovery Services

Implemented as part of the Data Center Framework, HPES' Disaster Recovery Management Services will provide strategy, process, type, methodology, locations, documentation and prompt restoration of the Services. Our solution is a subscription model, based on the County's currently-specified Recovery Time and Recovery Point Objectives. Applications with a 72 hour RTO will be recovered from replicated Virtual Tape Library (VTL) backups. Applications with a 48-hour RTO will have their DR servers mounted to replicated SAN storage. Under a subscription model, the server hardware "subscribed" to by the County is leveraged, provisioned with County images and applications on an as-needed basis to support DR tests, or actual disaster events. However, if shorter recovery times are required in the future, we can implement active/active and/or active/passive for web/Application/data layer recovery.

During transition, we will validate ongoing DR policies and procedures including:

- Portfolio Applications priorities and Recovery Time Objectives / Recovery Point Objectives (RTO/RPO) requirements
- Validation that restoration times meets County requirements
- The server strategy (subscription using replicated backups or SAN data, or one of the dedicated hardware options above)
- Data Synchronization and replication plans
- Rationalization of licensing costs

Our solution is based on F5 Global Traffic Manager (GTM) and Akamai. For active/active, should it be required, we would use a synchronization technology such as SQL server Always-on architecture or Oracle Data Guard architecture. Our technology Continuity of Operations (COOP) professionals, whose primary mission will be to build a robust DR program for the County, will write a viable and executable DR plan and will schedule and manage the DR exercises. Upon declaration of a DR event, HPES will execute the County Disaster Recovery Plan (to be developed during Transition):

- Recovering and resuming full operations including all supporting infrastructure and networks of:
  - County Requirements
  - Priority 1 applications within 48 hours
  - Priority 2 applications within 72 hours
- Recovering all County Data repositories with a data loss of no greater than 28 hours

Identity Access Management Services

HPES is dedicated to the Identity and Access Management (IDAM) security discipline that enables the right people to access the right resources at the right times for the right business reasons—while preventing unauthorized or intrusion attempts. HPES uses IDAM technology to initiate, capture, record, and manage user identities and their related access permissions. Our globally proven, fully automated approach makes certain that access privileges are granted according to a singular interpretation of policy and that all individuals and services are properly authenticated, authorized, and audited. Recognizing the critical importance of IDAM, particularly in light of emerging technologies and cloud-based infrastructure migration, HPES' expertise and experience in this area—combined with our familiarity with the County—enable us to offer an industry/enterprise-proven tailored IDAM solution.

HPES' approach to the County IDAM solution is to continue to evolve and improve the County's existing investments in PeopleSoft, Active Directory (AD), and Oracle IDAM to provide an overall platform to

protect and manage individual identities, their authentication, authorization and roles, and privileges. The starting point or foundational element of the solution is the Oracle IDAM platform, which is an industry-leading, end-to-end security solution—providing components that protect applications, data, documents, and cloud-based services through a combination of flexible authentication and single sign-on, identity federation, and risk-based authentication and authorization. The County's IDAM solution—starting with the Oracle platform and extending to the current County Active Directory, PeopleSoft, Public Key Infrastructure (PKI), Active Directory Federation Services (ADFS), and the HPES Identity and Access Management as a Service (IAMaaS)—provides an integrated, modular architecture. This architecture provides the County with the flexibility to deploy a complete solution that will enable the integration of current platforms, existing applications, and third-party security services into a single solution—offered at a single price point. We will implement IAMaaS post-Transition if optionally requested by the County.

The high-level scope of this solution is to use Oracle Identity Manager as the basis to manage the user accounts across various applications and integrate identities within Active Directory, PeopleSoft, the HPES IAMaaS, and third-party applications that contain County identities. The Oracle Identity Manager will act as a single point of user management for the administrator to create users and authorize the user to access the relevant resources across the County, while allowing the other key platforms that contain identities to continue. The Oracle Access Manager solution will secure the application access with respect to organization applications.

Reporting Management Services

HPES' solution and commitment will include the development, generation and submission of deliverables defined in Schedule 5 of the Agreement. HPES knows the current reporting criteria and will continue the current level of reports without interruption upon contract start. We will identify necessary reporting additions and enhancements to be completed as part of the overall Cross-Functional transition timeline. Through a coordinated effort, HPES will identify specific subject matter experts for each reporting requirement and match them with a County counterpart to make sure any new requirements are identified and supported for each of the Schedule 5 reports. In addition, HPES will demonstrate new and additional reports that the county may find valuable to manage their IT infrastructure as well as streamline the reporting process as new transition and transformation tools are applied. The implementation of HPES Service Manager opens up a new chapter on the availability for new and enhanced reports. The County will have near real-time reporting with fresh data to proactively monitor service performance and to take necessary actions. The HPES Service Manager provides 100+ out of box reports; intuitive UI helps to create easily navigable role-based dashboards to show only what is applicable to a particular role. Each report has the option of printing, exporting (PDF, MS Excel and HTML), Service Manager also has built in reports for KPI reporting.

Domain Names Management Services

The request for a new domain name (DN) and add-on DN services is initiated by the County Point of Contact (POC) via an IMAR request to the HPES Help Desk in myRequests or a project requirement. The Domain Name Administrator (DN Admin) will treat either request as authorization to purchase the DN and DN services from an accredited registrar/vendor.

The Help Desk routes the IMAR request to DN Admin who takes the following actions:

- The DN Admin checks DN Portfolio for an existing account for requesting department. If the requesting department has an account, the DN Admin uses the existing account for purchase or creates a new account if one does not exist.
- The DN Admin saves the confirmation receipt for future reference and adds DN and DN services to the DN Portfolio in the Integrated Asset Management System (IAMS).

- The DN Admin then emails the County POC confirmation of purchase and gives them an initial username and password.
- If the requested DN is not available, the DN Admin will email the requestor for an alternative DN.

The DN Admin is responsible for (i) actively monitoring renewal of DN and associated DN services and (ii) acquiring approval from County Point of Contact (POC) for renewal. The DN Admin takes the following steps for renewal:

- The DN Admin emails the County POC about DN renewal approximately 30 days before the expiration date. If there are DN services associated, DN Admin will also request DN services renewal.
- The County POC responds with approval to renew the DN. If there are DN services associated, the County POC will also indicate whether or not to renew DN services.
- The DN Admin pays renewal fees to the accredited registrar/vendor for the DN.
- The DN Admin updates the expiration date on the DN Portfolio accordingly and enters it into the IAMS.
- If the County POC decides not to renew the DM, the DN Admin will update the DN Portfolio in the IAMS

The County POC may request cancellation of Domain Name (DN) and associated DN services prior to its expiration. The DN Admin will treat these requests as authorization to release the DN name and associated DN services. The following are the procedures for cancellation of a DN:

- The County POC submits an IMAR-Remove ticket in myRequests.
- The Help Desk routes the IMAR-Remove ticket to the DN Admin.
- The DN Admin cancels DN and associated DN services with registrar/vendor and removes the DN from the DN Portfolio and saves the documentation in the IA

The DN Admin minimizes the number of registrars/vendors from whom they purchase DNs for ease of management and transition of services. The DN Admin purchases/renews DNs for no more than a 1 year subscription to minimize cost to the County in the event that a cancellation occurs.

The DN Admin will create an Annual Domain Name Management Plan that details all DNs in the DN portfolio, expiration dates of existing DNs, and any changes in DN Management procedures. The DN Admin will also create a monthly report that will include the following:

- Domain name
- Total quantity of managed domain names
- Quantity of new domain names added in the last month
- Quantity of domain names retired in the last month
- Quantity of domain names retained by the County
- Summary data for each domain name:
- Domain name ID
- Type / Extension
- Renewal Date
- High Org
- Low Org
- County POC Name, E-Mail and Phone
- Secondary County POC Name, E-Mail and Phone

Business Analyst Services

HPES understands that one of the most critical roles in the requirements management process is that of the business analyst. As such, the HPES solution includes establishing a team of Business Analysts to act

as a liaisons to the County Business Groups including LUEG, CSG, FG3, PSG and HHSA. These analysts will gather, analyze, communicate and validate requirements related to new IT projects or changes to existing applications, processes or policies. The HPES business analysts will engage all county and HPES stakeholders as well as contractor roles across the applications, engineering, testing, end-user support and security towers. Our solution recognizes the complexity of this role and provides tools for multifunctional teams.

The Business Analyst is responsible to articulate the county's high-level requirements for any IT system, and support development of those requirements for consideration within the scope of new development efforts. To do this, we will work closely with the County business owners and users. Business analysts have an advanced level of knowledge and expertise within the particular industry or client they support. We will field a mix of experts who know the county's business well, and are strong at eliciting and documenting requirements, as well as defining solutions. This hybrid approach to staffing Business Analyst Center (BAC) gives the County the optimal mix of knowledge of your business and functional/technical expertise from outside the county. The benefits of our implementation of the BAC include;

- Flexibility in the business analyst staffing arrangement. Analysts will be available through a pool of resources the county can utilize on request or exclusively through a level of effort (LOE).
- Shorter delivery time to meet customer demands. As the county has direct contact with HPES business analysts that can act as a bridge between requirements definition and solution development, they can improve and enhance service delivery to their employees and constituents.
- Experience in aligning the right resource to the right effort. Previously the County had experience with Customer Solutions Advocates who were dedicated to the County business groups. CSAs had intimate knowledge of the business groups in which they were assigned and provided business analysis services to the business groups when solutioning and assisting in solving business problems.
- Continued engagement throughout the project lifecycle. Business Analysts will participate in post-requirements phases, for example guiding User Acceptance Testing and acting as Training and Documentation SMEs.

To support the solution, HPES will leverage our Enabling Delivery and Global Excellence (EDGE) methodology and toolset to develop the standard processes that the team will follow. EDGE is a repository of best multi-functional methods, tools and processes that will inform the creation of a custom, repeatable solution that is right-sized for the county of San Diego.

The primary change improvement will be the deployment of a new County Enterprise Portal which will provide a common point of access for all County information. There service desk will be enabled with an upgrade from HP Service Center to HP Service Manager. This upgrade will provide an extensive improvement to not only the help desk but other County Systems which integrate with Service Manager.

Competitive Differentiators

In addition to the leading edge technological excellence that HPES provides, as corroborated by the Gartner Group, we are first and foremost a dedicated partner to the County of San Diego. We have a rich history of working together and mutually enjoy relationships based on trust, openness and competence. We share the County's long-term goals and vision, as we are ingrained the County culture, its residences, and evolving needs.

HPES provides the County a unique differentiation; to leverage your existing investment, provide a low risk solution while providing solutions that position the County to benefit from future technology enhancements. We will continue our record of meeting County IT services needs as we explore, recommend and implement new and exciting innovations.

County Benefits to Our Proposed Solution

- Leadership who understands the County needs
- Low-risk
- A customer-centric mindset, "Demonstrate you care!"

2.6 Service Desk Services Framework

Executive Overview

End-user satisfaction with Service Desk for the County is an HPES imperative. A responsive Service Desk requires agents to know the County business and understand the importance of resolving issues and processing service requests (SRs).

HPES Service Delivery Reliability

"...[C]ustomer service and account team is very sensitive to the client's needs, and is able to meet service levels consistently. References also praised the ability of HP's service team to prioritize a customer's productivity."

2015 Gartner Magic Quadrant for End User Outsourcing Services, North America

042 CA CoSD

As the incumbent, we have deep knowledge of the County IT infrastructure and mission. The County Service Desk will serve as the single point of contact (SPOC) for the receipt, logging, classifying, prioritizing, tracking, resolution, and reporting of incidents and SRs for End Users. Service Desk will accept contacts by phone, email, chat, fax, and portal and will route tickets to the appropriately skilled and available Service Desk agent, who will provide first-level incident resolution. If an incident requires additional troubleshooting, Service Desk will escalate the ticket to the appropriate resolver team for action and resolution.

Our approach to resolving incidents and SRs is to manage them from initiation to completion in a closed feedback loop process that takes into account lessons learned based on 10 years of Service Desk support to the County. It combines ITIL-aligned industry best practices, an up-to-date knowledgebase, clear resolution scripts, agent training and development, and regular ticket feedback reviews. HPES plays an active role in continuously improving Service Desk responsiveness, customer service interactions, resolver scripts, technical expertise, and End-User satisfaction.

The County's environment is ever changing, and we will evolve and adapt support as required. After implementation of new technologies during Transition—such as the HPE Service Manager (HPSM) system and the Service Portal—we foresee an improvement in our ability to standardize the collection of data on Service Desk; collect more categories of data, including on customer satisfaction feedback; and post service-level data to the Improve first-call resolutions, recognize the most frequently asked questions (FAQs) and develop effective answers for the portal's knowledgebase, and develop the most effective types of customer feedback.

HPES has a successful record of implementing Service Desk self-help technology and processes (see Qualifications and Experience). We will use our lessons learned drawn from these engagements and from County input to document and maintain self-help procedures, including for password reset, SR entry, tracking, reporting, updating, and status checking, which will support the new Service Portal. We will align the self-help procedures with County policies and submit them for County approval.

HPES is dedicated to continuous service improvement in our Service Desk response to users and in swift resolution of incidents and fulfillment of SRs. We look forward to implementing the County's vision for Service Desk on the new contract.

Service Desk Services (Schedule 4.3, Section 3)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The HPES Service Desk for the County serves as a single point of contact and the primary owner for monitoring and tracking of all incidents and SRs for approved end users. Our key solution strategy is to use ITIL-aligned processes to meet requirements, achieve 70% first-call resolution (FCR), and achieve 12-minute phone handle time as well as Service Desk ownership for end-to-end tracking of all tickets and SRs. Our Service Desk uses knowledge documented in the electronic Knowledge Management System (EKMS) to make a swift determination on whether an issue should be warm transferred to our remote

desktop/device management (RDM) capability or escalated to deskside/field support or the appropriate framework (e.g., Applications M&O, End User, Network).

Our updated training processes provide agents with in-depth knowledge of County processes, scripts practice, and ITIL-based practices. We make sure all employees including new hires receive our Doing Business with the County instruction and monitor individuals for its completion. We integrate the training activities our agents receive with real day-to-day work assignments. Our training increases agent comprehension of County-specific issues and expertise in routing tickets efficiently and effectively to the appropriate technical support group. It improves agent communication skills when in contact with end users by phone and email—and by chat upon its implementation. It also helps us to more effectively meet the County requirements and service levels. We also will identify those agents who require additional instruction and customize training to strengthen their skills.

Service Desk Agent Training for Continual Service Improvement

Incorporating lessons learned, HPES will take the following measures on the new agent contract hires

- Make "Doing Business with the County" training mandatory for all existing and new hires
- Change annual review to quarterly reviews of Service Desk scripts by Training Analyst and Knowledge Content Analyst to ensure language and content that agents are using is effective with callers and resolution of issues
- During Service Portal implementation, train agents in new modes of receiving/dispatching tickets, chat functionality, and understanding of user self-service

149 CA CoSD

As we implement the self-service technologies on the new contract, we will encourage users to access the Service Portal's self-service functionality from their desktops, tablets, or mobile phones. We provide our technology End-User adoption approach in our response to Section 2.6.1.7.

Our HPSM system's data analytics functionality will include documentation and display on the Service Portal of Service Desk statistics tied to both our team's objectives and the County's service levels. Along with call data, this will enable our Service Desk manager to perform quality reviews on relevant areas such as call waiting/call abandonment, efficiency in meeting the phone time to resolve metric, rate of FCR success, and End-User satisfaction levels upon ticket resolution. On systematic review of trends, surveys, and reports, the Service Desk manager, together with other members of the HPES account management team, will find opportunities for improvement of Service Desk services and operational cost efficiencies.

Service Desk Structure

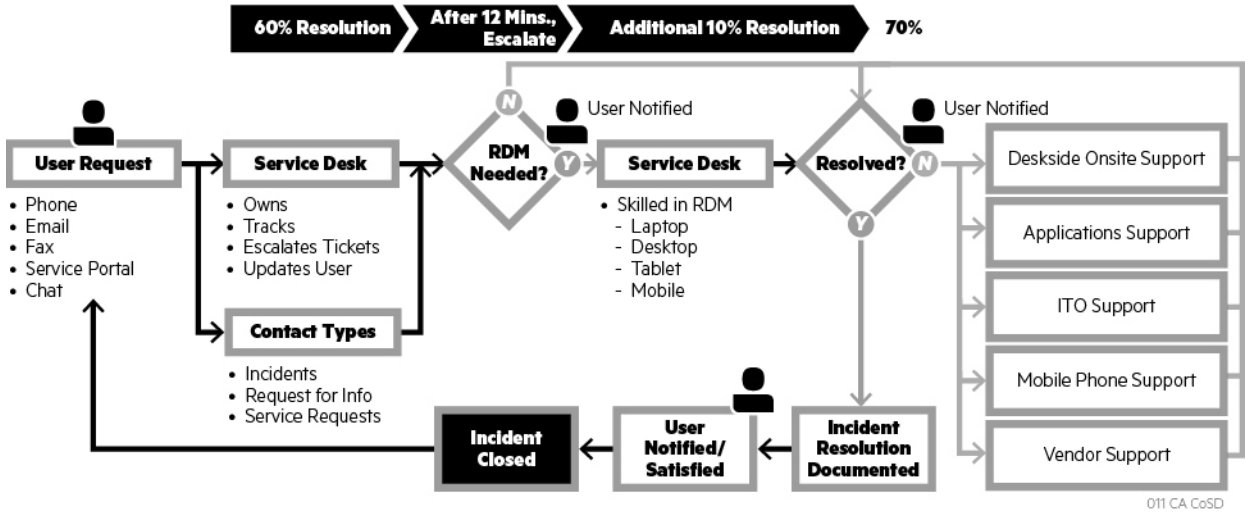
Service Desk. The HPES approach to Service Desk is rooted in the ITIL framework, focusing on repeatable, scalable processes and continual process improvement. In Figure 37, we show the Service Desk full life-cycle ticket ownership and end-to-end tracking of all incidents and SRs for all County End Users as well as all other authorized contractors and stakeholders.

Our ITIL-aligned methodology for service delivery focuses on providing a high level of customer satisfaction, maximizing first-call resolution, and taking ownership of SRs and incidents. As the current provider of Service Desk services to the County, our approach is supported by agents who are the first point of contact and if needed provide remote desktop/device management (RDM). If support requests cannot be resolved by the first contact agent (Level 1), then the call is escalated to RDM (Level 2). In some cases, the Service Desk agent will need to escalate to the deskside/field team or subject matter technical support (Level 3), which includes frameworks such as applications, engineering, exchange, data center, infrastructure, storage, etc. Level 1 and Level 2 resources will primarily reside within the Service Desk Framework unless local support is required/requested or a lower-level issue is called in that requires subject matter expert (SME)-specific support—for example, a single user mailbox restore. Level 3 support will be provided primarily by the various frameworks mentioned above unless the Service Desk has the ability to resolve the issue based on the documentation provided by the framework and has the required access to the systems. Service Desk training and detailed documentation outlining the correct escalation path for each type of incident or SR will guide agents to make certain that tickets requiring escalation are routed correctly the first time.

While the Service Desk Framework is responsible for the full life cycle and management of all incidents, IMARs (installs, moves, additions, and removals), and SRs, each framework is responsible for management of their work stream, making certain that work is triaged within the required timeframes. Points of contact (POCs) are identified within each group to manage these activities and verify work is completed. Costs associated to these activities outside of the Service Desk agents will not result in additional costs to the County.

Remote Desktop Management (RDM). The primary function of RDM is to allow the Service Desk agent to provide a higher level of technical service, handling problems and issues that may require technical resolution. Using RDM for remote tool capabilities, a Service Desk agent can interact with network services, software systems engineering, and/or an applications group to restore service and/or identify and correct problems. This may require assisting in simulation and recreation of user problems and recommending systems modifications to reduce user problems. Service Desk agents will be facilitators between customers and other support teams to make certain customer needs are met and tickets are resolved in an expeditious manner.

Figure 37. Comprehensive Service Desk for the County



Our simplified workflow increases first-call resolution rates and decreases Tier 2 dispatch to County sites.

We will continually add to the knowledgebase, working closely with other resolver groups to identify areas where we can improve knowledge documentation to provide increased resolution at first call, freeing resources to support their other activities.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Resource Management — Oversight for Service Improvement. The Service Desk manager will be responsible for providing oversight of performance, resource management, and service delivery, including the collection, consolidation, and dispatch of events and information sent by the County as it relates to the environment. An important part of this role is to review metrics on customer satisfaction and success in meeting County requirements and establishing quality processes and intensified training approaches to improve Service Desk performance. Our reporting analyst will analyze Service Desk data, identifying and adjusting metrics queries, and fulfilling the ad hoc Service Desk-related report requests from the County and from the HPES service delivery manager in the County.

The Service Desk manager will lead daily status calls with the workflow manager, operations manager, and shift leads to make announcements, communicate County concerns, and review the status of any issues that emerged overnight. In addition to the daily status calls, the Service Desk manager will call meetings every Monday before each shift begins that include the agents on deck. These meetings will provide a venue for management and agents alike to raise issues they would like addressed and to foster interaction with the Service Desk manager in his efforts to support alignment with County expectations. Our Service Desk support concentrates agent numbers in shifts during the County's core hours from 6:00 a.m. to 6:00 p.m. PT, Monday through Friday, and maintains support overnight and weekends.

The workflow manager will support the Service Desk manager in providing day-to-day supervision of operations, monitoring that agents arrive on time and are attentive to their responsibilities, adjudicating rotation of shift personnel, and making sure that the metrics gathered on Service Desk are uploaded properly on the Service Portal for review by the Service Desk manager, the quality analyst, the HPES account team, and County administrators. Important to this role, the workflow manager will constantly communicate with the Service Desk manager, updating him on Service Desk issues throughout the day, workloads, and staffing, including issues of individual agent performance.

Working with the operations manager and scheduler, the shift leads will monitor the ticket queue to make sure tickets do not go unattended. Other shift lead responsibilities include providing oversight of ticket agents' handling of Priority 1 and 2 Incidents and VIP/Critical User tickets. Our shift leads oversee agent performance and work with the Service Desk's training analyst to develop measures to improve expeditious handling of tickets and effective agent–End User interaction. Our training analyst will check the training history of individual staff, making certain that all staff take our mandatory training, and will provide follow-up as necessary.

Service Desk escalates tickets to our technical support groups located at the County Administration Center (CAC), County Operations Center (COC), the HPES Rancho Bernardo facility, and the AT&T location on Trade Street. We discuss resource management and facilities in Section 2.07.1, End User Services.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The County's environment is ever changing, and we will change to continue to assist in moving the County forward. We understand both the importance the role of the Service Desk has as the first contact for the County and the need for agents to be up to speed to remain aligned with the County's business.

IT Service Management (ITSM) Processes for Service Desk. HPES implements ITIL/ITSM processes for Service Desk with a focus on customer service satisfaction and continuous improvement. For example, keeping End-Users updated on ticket status is an important element of customer service. As a key ITSM framework process, our Service Desk owns and tracks tickets created at initial call or are assigned via the Service Portal, and it is their responsibility to maintain open communication channels with the user in the event of a ticket inquiry throughout the ticket's life cycle. Our system enables us to expand the platforms for End-User communication to mobile devices, portal notifications, chat, and email. Integrated with other service management disciplines in HPSM, our Service Desk agents also provide an interface for activities such as SRs, customer change requests, incident management, and third-party support.

Continuous Improvement. ITSM processes support continuous process improvement based in data collection through the Service Desk system, Customer interactions, HPSM, the Avaya CMS Call Manager, and the Customer feedback surveys that we upload for data aggregation and review. All of the data input from these systems—along with the additional reporting that we will be adding from chat and

Self Service—will be placed into the analytics environment that will be created in support of the Service Portal to make certain that we are continually focusing ways to improve our support, technologies, and staff to provide the best possible service to the End-Users. Service Desk related data will be posted to the Service Portal and reviewed regularly with the CTO during the Operations status calls. The detailed process of the approach we will use is provided in Service Desk Specific question 2.6.1.10. Past continuous improvement review and input from CTO provided the catalyst that compelled our team to transition to a more effective customer survey, upon approval by the County back in 2011. The sample we provide in Section 2.6.1.1 has proven its effectiveness in assessing user satisfaction at the HPE Global Help Desk; it is the same survey HPE employees receive worldwide.

Our ITSM-based processes focus on improving agent performance and therefore customer service. In the following section, we discuss management and training processes that result in higher levels of customer support.

Quality Monitoring to Improve Agent Overall Performance and Customer Service. Our approach is to engage each agent of the Service Desk team to participate in developing strategies for improved customer service. Our Service Desk manager together with the workplace manager and shift leads will review the results of the customer satisfaction surveys and other relevant data displayed on the portal (for example, phone handle times at initial call, ticketing information, chat data, most common scripts used, etc.) to discover areas for improvement, discuss them with the quality assurance (QA) analyst for Service Desk, and present findings at a Monday all-hands Service Desk meetings for each shift.

At these meetings, managers and leads will make recommendations on issues identified or for the agents to raise new problem areas they have experienced the previous week. The workplace manager uploads results and new resolutions from the meeting to the Service Desk dashboard reserved for agent posts. As each shift conducts its Monday meeting, additional comments are added to the dashboard. Not only will these recommendations be used to improve the support the agents are providing but will also be communicated by the Service Desk Manager to the CTO where applicable where we may want to enable new tools, processes, and so forth, to improve overall service and reduce the volume of calls.

Consistent quality monitoring gives agents ongoing coaching and feedback on their performance and the opportunity to increase their customer service skills. Our four-step quality management framework, supported and documented by our QA analyst, is: (1) Monitor Performance; (2) Analyze Performance; (3) Identify Areas for Improvement; and (4) Establish Corrective Actions 5) Verify Improvement. The framework aligns with our seven-step ITIL processes for continuous service improvement discussed in Section 2.6.10.

Monitoring Performance of Individual Agents. We capture agents' voice interactions with users along with the corresponding computer desktop activities, such as data entry for logging tickets, cataloging and prioritization, screen navigation, and data retrieval from the knowledgebase. To effectively coach employees, we use two quality monitoring methods: side-by-side and remote. In side-by-side monitoring, the shift lead uses a headset to join the call of a new agent or an agent learning better communication skills. The shift lead also uses remote monitoring—that is, agents are unaware they are being monitored—to audit and evaluate agents' performance for our quality metrics.

Our Service Desk manager consults with the workplace manager and shift lead to perform agent evaluation review and identify patterns to assist agents in understanding how each aspect of their performance affects the whole.

For agents falling below the satisfactory level, the workplace manager and the shift lead pinpoint the issues that need improvement and develop a Performance Improvement Plan (PIP) with the agent that addresses the areas of poor performance. For example, agents having difficulty resolving a sufficient number of tickets within the 12 minute handle time receive additional playback training to gain an

understanding of the process. The Service Desk manager will deploy our training analyst as necessary to review findings on individual agents' performance and help develop customized training to address these issues.

- Automated Tools – Automated systems and tools involved in proposed solution

We are implementing for the County HPE Service Manager (HPSM), our system that includes comprehensive core and extended Service Desk advanced functionality. It provides key Service Desk automated processes and the capability to manage our responses to County users, including FCR, deskside support coordination, and ticket and SR escalation to support, including to AT&T network/mobile SMEs and other vendor support.

We are confident the County will be enthusiastic about our system's Service Portal and its self-service capabilities that we are rolling out within 90 days of contract start. The portal implementation approach as detailed in the Transition section for the Service Desk will include the core functionality of new services and links to current data sources and source systems to integrate with current repositories within the 90-day timeframe. At the end of the transition period users will be able to perform the following via self-service:

- online ticket creation
- Review/status of tickets and Service Requests
- Perform online password resets via the Self Service Password Reset, SSPR tool
- Conduct chat sessions with the Service Desk for information or support
- View reporting
- Access to the Knowledgebase (FAQs, tips sheets)
- View Outage Status, Trending Now, and Announcements
- Access to MyRequests, and various links (ITSC, DocVault, etc.)

The new service catalog that will replace myRequests and the complete integration of the configuration management systems (Asset Manager, Apps Manager, ESL) will be implemented as a part of the transition and is included under the Cross functional transition section and timeframes. Further information can be found in Section 2.11 Transition Services Framework, 2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5), Special Cross Functional Project – Replacement of myRequests. We will engage the CTO, framework administrators, and other relevant County stakeholders to provide input into the look and feel of the portal. Our sample portal landing page in Figure 38 demonstrates that County users will be able to access the Service Portal, including self-service functionality, from their desktops and other platforms.

On-Going Maintenance, Support, and Enhancements: The Service Desk Manager will be the primary point of contact for the Service Portal for the County of San Diego. Technical support and enhancements will come from the Portal framework, which is a leveraged team much like the resources that we use in our data centers and other frameworks today. The Service Desk Manager will be responsible for making certain not only that issues related to the portal are being resolved but that maintenance items and new features are being implemented as needed.

The Service Portal has a quarterly maintenance schedule that the team uses to address issues and add new features. We will follow this maintenance schedule for changes to the portal that are non-incident related and for changes that may require coordination, training, and communication to the End-Users. Simple

changes (adding links, contacts, FAQs, Announcements, Trending Now information, etc.) will take place on a frequency agreed with the County that we will discuss during Transition planning. The overall focus around the processes and frequency related to these changes will be to ensure the latest and most accurate information is published to the portal in a timely fashion to benefit the End-Users. Once the timelines are established, processes will be built, approved and communicated as required. To make certain that the changes being made are communicated, well thought out, and in the best interest of the End-Users, the Service Desk Manager will be a part of a Portal Review Board the final composition of which will be established by the CIO in consultation with the Contractor Account Executive. to discuss, approve, document, and communicate all changes related to the Service Portal. These changes will include not only the content within the Service Portal but the processes related modifications that need to be made over time to ensure information and Service Portal accuracy. For changes to the Service Portal that require Portfolio Application modifications or County data manipulation, a BE will be provided to the County to determine how or whether to proceed with these changes.

Training: Training will be provided for all End-Users and support staff as a part of the Transition project related to the Service Portal. This will cover every aspect of what will be in place at the end of this project. As a part of transition planning, we will discuss with the County the various training options and communications that will be needed to ensure that all County End-Users understand the capabilities of the portal and how the portal works.

Figure 38. Sample Landing Page for Service Portal with Self-Service Functionality

060 CA CoSD

We anticipate the County IT Architect and other County stakeholders will provide input on the design of the portal.

County users will be able to click a tile to phone Service Desk, open a ticket on their own, reset their own passwords, make SRs, check County announcements, access training, FAQs, and Tips, and stay alert to outages. For example, the tile for SRs, as shown in the Figure 38, will invoke myRequests, as would other select tiles, such as Service Catalog. In another example, upon clicking "Open Ticket," a dropdown menu appears that allows the user to select from a list of problem categories; once the category is selected, a second dropdown menu appears with category-relevant problem descriptions. During the process, if the user decides guidance is needed from a live agent, he or she can click the "Chat" tile or "Call Service Desk" for support.

County Call Abandonment Rate

For County of San Diego, HPES implemented, operates, and maintains three enterprise service desks that handle an average of 10,000 calls per month and provide a single point of contact for users. Through process improvement, we have reduced call abandonment rate to 3 percent of all calls.

044 CA CoSD

When a ticket is created from the portal or the Service Desk via a phone call or email, Service Desk embeds the user's profile (i.e., contact information, location, and asset information) in the ticket and tracks it until resolution, posting updates on the ticket's progress on the portal. This allows the user to easily obtain ticket status by accessing the portal landing page from his or her desktop, tablet, or mobile phone, as we discuss in Section 2.6.1.6.

When phase-in is complete, our plan is to migrate myRequests to the HPSM system that will help us obtain more accurate data for aggregation, review, and input into monthly reports to the County.

Service Request Management Services:

Our solution is to provide Service Desk agent assistance for fulfilling Service Requests (SRs) and to enable users to create their own SRs on the electronic processes of the Service Portal's self-service capability. Our Service Portal will use HPSM and myRequests, the current application for SRs and ticketing, that will provide the entry point for other tools such as SharePoint. As part of the Cross Functional Transition phase, we will migrate myRequests to HPSM's more advanced SR functionality. We will initiate and execute this project and its design at a time expedient to the County's priorities.

We will work with County framework administrators to capture and document all SR-related content and maintain it in a rules-based database within the SR Management tool. We also propose to develop a Service Portal version of the OIC Service Catalog.

Service Desk Agent SR Assistance. Our Service Desk agents currently assist users with submitting SRs for items such as installs, moves, additions, and removals (IMAR) or changes to the workplace environment.

Service Desk will continue to provide this service, by creating records on SR forms, copying an existing record, or applying a predefined template that prefills specific fields using electronic processes:

- The user makes the SR to the Service Desk by phone, email, fax, or the Service Portal.
- The Service Desk agent determines if the SR is a request or an Incident and follows a closed loop process
  - If the request is an Incident, it is handled as discussed in Section 2.6.1.
  - If the request is an IMAR, the agent will refer to the appropriate documentation to make certain that the request is routed properly to the appropriate framework. Details of this process are provided in Section 2.7 End-User Services Framework - IMAR
- The Service Desk agent categorizes the request and assigns a priority level.
- The Service Desk checks the Service Catalog, which is based on the OIC Service Catalog, to determine if the SR needs approval and, if so, the level of approval required.
- If a request is approved, the Service Desk agent escalates it as appropriate, and updates the user upon request.

Service Requests by Self-Service. Once the Service Portal is implemented, the user will be able to make SRs on user-friendly SR forms that are routed to the Service Desk ticket screen (in accordance with the approvals granted by the County). A Service Desk agent will be assigned the SR that arrives from the portal and will review it and follow predefined steps in a workflow, including classification, fulfillment, and validation.

Service Portal Service Catalog. We propose developing a version of the OIC Service Catalog suitable for Service Portal self-service. We envision the portal's version of the Service Catalog to be accessible to all End-Users for making Service Catalog-based SRs. The SRs will display the approval process required to the user before being routed to the Service Desk. A Service Portal version of the Service Catalog will provide the following benefits:

- Reduces Service Desk's workload by providing self-service capabilities for Service Catalog requests that flag approvals that are required
- Ensures all self-service SRs are routed to Service Desk for review
- Provides a single, guided, questionnaire-style user interface for requesting support for catalog and non-catalog items

- Provides tablet and mobile user support.

- Qualifications and Experience – Background and experience in comparable environments

HPES supports approximately 5.4 million desktops for more than 550 clients in more than 135 countries, and we continue to be recognized as a Leader in Gartner North American and Western Europe Desktop Outsourcing Magic Quadrants:

GSA: Through the Integrated Acquisition Environment (IAE) Federal Service Desk (FSD) contract, we supported GSA in creating a contact center for Tier 0 (self-service) and Tier 1 services. Under a new task order (TO), we continue to support Tier 0 and Tier 1 services as well as Tier 2 services. The call volume is 70,000 per year.

E.ON: Through an IT Outsourcing contract, we helped this client to consolidate nine local service desks by leveraging skilled resources with the necessary language skills into a four-site, integrated global support center from which we provide onsite support and 24x7 service desk support for more than 80,000 employees worldwide. There has been a 15% reduction in manual service desk. First contact resolution scores at E.ON exceed industry expectations and support user productivity. User satisfaction scores are 90%+ based on efficient and timely support for the IT workplace. The call volume is approximately 150,000 per year.

U.S. Citizenship and Immigration Services' (USCIS) National Customer Service Center (NCSC): HPES transitioned support for the NCSC and assumed more than 200,000 calls per month from the incumbent vendor. This startup included two locations—an existing subcontractor facility and a specially constructed HPES facility. HPES acquired and built out new facilities, implemented DHS-specific systems at both locations, and arranged for the installation of DHS OneNet connectivity. Services were transitioned on schedule without disruption.

HUD: Under the HUD Information Technology System (HITS) contract, we helped HUD eliminate redundant service centers, reduce costs, improve service levels, and reach a single point of contact (SPOC). We provide a nationwide service center that supports desktops and field services through a SPOC. The service center supports approximately 14,000 HUD users and several thousand HUD contractors and external business partners in more than 80 locations throughout the U.S. and its territories. We have consistently achieved customer satisfaction levels of 95% and higher, where users rate our services as good or excellent. The call volume is 186,000 per year.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP

None.

2.6.1 Service Desk Services Specific Questions

2.6.1.1. Describe your approach to ownership and end-to-end tracking of Incidents

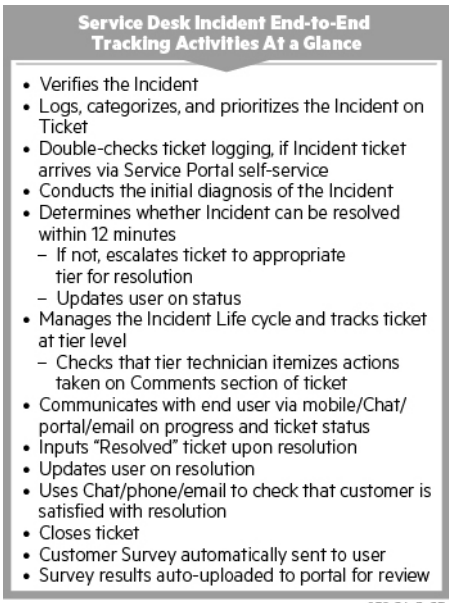
Service Desk has ownership of all tickets and tracks them from user submission through ticket resolution. We have implemented ITIL-aligned processes enabling any Service Desk agent to check on ticket status even if it has been escalated to other resolver groups for action. The Service Desk agent can also update the user on ticket progress until it is resolved. Service Desk's continuing involvement in ticket progress makes SPOC meaningful to the end user. These processes have been in place since 2006 developed in collaboration with the County. We are updating and adjusting these processes, such as the root cause analysis (RCA) process on Incidents and Problems, with the County, as required, to make sure we continue to improve service.

The following section focuses on Service Desk ownership and end-to-end tracking of Incident tickets.

Service Desk Handle Time and Escalation of Incident Tickets. When a user calls in an Incident by phone, the Service Desk agent who answers the call owns the ticket. The agent first verifies whether the call is for an Incident rather than a Service Request (SR). Once an Incident is validated, the agent logs the ticket, including the user profile, categorizes the Incident, and prioritizes the ticket according to the County's priority matrix (i.e., Priority 1–3); if the caller is on the VIP list, the user profile automatically alerts the agent to register the ticket as Priority 1 or 2 depending on the severity of the issue.

Should the Incident arrive through a user-created ticket via the Service Portal, its automated processes upload it to the ticket queue for selection by available ticket agents. Ticket assignment order is determined by first in/first out and by severity. Severity 1 and Severity 2 tickets receive immediate attention by Service Desk agents, with oversight by the Workflow Manager and Shift Lead.

Once the Incident is logged, the Service Desk agent assigns the ticket, starts troubleshooting, and diagnoses it using information provided by the caller or the description on the portal-generated ticket. The Service Desk agent can quickly resolve low-level Incidents associated with known errors by applying approved solutions or workarounds. In other cases, the Service Desk agent may know immediately that the Incident cannot be resolved and will determine, based on knowledge documented in the EKMS, whether it should be routed to deskside/field support or to the appropriate framework (e.g., Applications M&O, End User, network (AT&T)) for resolution. In some cases, vendor-specific support may be required. The knowledge incorporated in the EKMS derives from information provided by the vendor on its hardware/software; resolution and workaround instructions developed by our SMEs based on their respective areas of expertise (e.g., applications, network); and information developed by the County SMEs on its infrastructure.



Deskside Support Escalation. When our deskside technicians receive a ticket, they retrieve all the service attributes from the EKMS and launch scripts and perform progressive troubleshooting based on the documented knowledge to identify the probable source of a service Incident. For example, if Service Desk performs troubleshooting and is unable to resolve the ticket, the Service Desk agent itemizes the actions taken and issues still unresolved on the ticket's Comments section. Service Desk notifies the user that the ticket needs further troubleshooting deskside; the technician coordinates the date and time for the visit with the user and posts the appointment in the ticket. The ticket information, including scheduled deskside visit, is viewable via the Service Portal.

Subject Matter Expert (SME) Escalation. When the Service Desk agent recognizes that the source of the Incident requires SME support, he/she escalates the ticket to the SME support team appropriate to the affected framework (e.g., Applications M&O team, Network team).

In addition, Service Desk escalates unresolved "child" tickets that match a "parent" ticket to the SME support team working on that Incident's resolution. The SME support teams perform additional diagnostics, as necessary, to identify and implement an appropriate solution or workaround. These teams take a comprehensive approach to resolution, keeping in mind the parent/child ticket linkage and recording their actions in the Comments section of the ticket accordingly. Once the issue is resolved, the Service Desk updates the status of all the linked tickets on the Service Portal and notifies all impacted users.

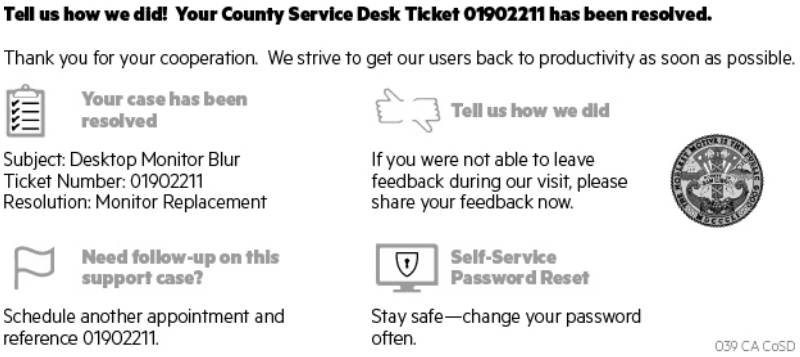
Vendor Support Escalation. When a ticket is escalated to a third party (i.e., vendor) regarding a product that cannot be resolved by our deskside technicians, the Service Desk ticket owner confirms that the problem is fully described on the ticket before it goes to the vendor's helpdesk.

Ticket Closure. Once the ticket is resolved, the resource responsible for the resolution changes the status of the ticket to "Resolved." This action automatically notifies the user via email of the resolution, as shown in Figure 39. The body of the email requests a reply within 3 days if the issue was not resolved to the user's satisfaction. If no answer is received after 3 days, the ticket status remains "Resolved" for an additional 7 days in case the user is out of the office. If the user does not reply after the additional 7 days, the ticket is automatically set to "Closed." HPES will continue using this format to update the user on resolution if desired by the County, but we propose a more effective verification email shown in Figure 40, as part of our continuous service improvement efforts. The benefits of this email are that it shows the user how the ticket was resolved and encourages, encourages the user to complete the customer feedback survey, and promotes the County's self-service password reset requirement. When the user clicks on the respective blue icons in this message, he/she goes to the Service Desk site related to the text.

Figure 39. Ticket Resolution Update

Currently, users are informed of resolution by email, asked if they agree, and encouraged to access the customer feedback survey.

Figure 40. Sample Incident Resolution Update to the User



Our message encourages the user to rate our service, indicate if they are not satisfied, and to support cybersecurity by changing his/her password.

The "Tell us how we did" icon leads to a customer satisfaction survey that provides a field for the user's email address. The Service Desk agent does not see the customer survey upon its return through our automated processes, but rather it is uploaded on our HPSM for data aggregations for Service Desk Manager review.

2.6.1.2. Describe your proposed approach to maintain and refresh Service Desk scripts.

We have developed structured formats for receiving calls and scripts that have proven successful in addressing problems and accelerating resolutions within 12 minutes on Service Desk. Scripts specifically tied to RDM and higher-level technical solutions support Service Desk technicians, deskside technicians, and SME support groups (e.g., Applications M&O, End User, and AT&T network). These groups develop scripts and work instructions for their own respective use in working infrastructure, applications, and network tickets. When the County users request a new script or a modification of a current script, the appropriate technical support group communicates with them in developing the script in adherence with CoSD-170 Help Desk Script Revision Process.

Our knowledge content analyst for Service Desk reviews scripts for consistency with the database methodology and style guide, recognizing that certain Service Desk scripts are spoken to the caller. We maintain successful scripts in a Service Desk EKMS with rules-based access to our agents/technicians. Our Technology Refresh team refreshes EKMS and the Self-Service Knowledgebase annually.

Our Service Desk Manager will adhere to the Framework Revision Process flow established by the County and post our Monthly Revised Scripts—Revision/Acceptance Report, which enumerates the total scripts in the EKMS and the number of revisions that month.

Using HPSM, we can collect metrics on response and resolution times associated with respective scripts that our agents use against identified problems. In addition, our Service Desk Monday meetings with the team are important as agents raise issues that have emerged using certain scripts, while highlighting those scripts that have proven to be effective.

In reviewing metrics and issues raised by our agents, the Service Desk Manager will identify less helpful scripts and assign them for rework. Our development of new scripts or revisions of existing ones will draw from the HP Global Help Desk scripts, a database of proven scripts to address a range of problems that have demonstrated success on our accounts worldwide.

Our Service Desk will support the Service Portal by reviewing the scripts in the EKMS and selecting those appropriate for revision for "how to" instructions with visual aids for upload into the Self-Service Knowledgebase. We will work with relevant SMEs in developing suitable language for End-Users accessing the Service Portal's self-help functionality. This will include tips, training and FAQs.

Scripts are important, but they are not a substitute for dynamic interaction with the user. Our approach is to use scripts as guides and to train our Service Desk agents to avoid giving robotic instructions to the user. Our training includes shift leads listening via headphones to agents using scripts to provide practice reviews and quarterly reviews of our training processes by the training analyst.

2.6.1.3. Describe your proposed strategy for preventing abandoned calls, including examples of where this strategy has been successful.

The keys to preventing abandoned calls are: providing agents with training and tools to resolve a ticket or escalate the issue quickly, reducing the volume of calls by introducing a Self-Service Knowledgebase through the Service Portal, and staff appropriately to handle peak demand.

Service Portal: HPES' experience in implementing Service Portals enables us to reduce ticket volume, thus freeing agents to answer initial calls more quickly.

Service Desk Agent: Our Service Desk agents have objectives to of 12-minute resolution times and 70% first call resolution. The faster the Service Desk agent can resolve the call or route it to other resolver groups, the more live agents will be ready to take the next call.

We will increase our training of Service Desk agents, both new hires and incumbents, to increase their ability to resolve tickets quickly. This training will include our indexed Knowledgebase and scripts to resolve less complex Incidents quickly at first call. For callers making SRs, the trained Service Desk agent will be able to point the caller to the related content in the Service Catalog for products and direct the caller on how to use the SR tool on the Service Portal.

Additional Measures: We take measures that shorten the phone handle time to restore service to the user as quickly as possible and allow the agent to help the next user.

- We provide our agents with a Self-Service Knowledgebase with an indexed search engine at their fingertips; this capability gives the agents confidence in their response and consistency in their answers
- Our agents open their response to the caller with a time-saving structured format (template)
- The call waiting recording provides the option for the user to leave voicemail that will be returned within 15 minutes

On our current County engagement, our Service Desk handles an average of 10,000 calls per month. Through process improvement, as shown in Table 23, we have reduced the call abandonment rate to 3% of all calls, which is 2% below the industry standard of 5%.

Table 23. HPES Call Waiting and Call Abandonment Rates.

MASLS 2015	DEC 2015	NOV 2015	OCT 2015	SEPT 2015	AUG 2015	JUL 2015
Call Waiting 90%	93%	93%	95%	96%	77%	94%
Call Waiting 96% / 3%	97% / 3%	97% / 2%	98% / 2%	98% / 2%	86% / 4%	98% / 3%
Call Abandonment <5%	3%	2%	2%	2%	4%	3%

HPES' call abandonment service level currently exceeds industry standard.

2.6.1.4. Describe your proposed first call resolution strategy. Include tier support escalation and retaining ticket ownership and oversight

Seventy percent (70%) first-call resolution rate (FCR) is the industry-accepted service level. Gartner reports, under Service Desk Statistics on FCR, 2014, the industry average has dropped to 63%. Indeed, HPES' review of Service Desk statistics in general found that once self-service is introduced, FCR falls because the overall ticket volume decreases resulting in an increase in the proportion of tickets requiring SME support.

HPES has developed an innovative feature of our Service Desk structure to meet 70% FCR. Upon receiving a call, the Service Desk agent accesses the Service Desk module's dropdown menu, which provides a range of predefined problems or SRs; this menu format saves time ordinarily taken to develop a description of a problem or SR.

A Service Desk agent quickly assesses the issue and determines if it can be resolved by the agent or must be escalated for SME support.

- We will identify data in HPSM to determine overall FCR performance, by contact type and agent identification.
- We will calculate the number of repeat calls on the same issue to identify trends and problems and develop Knowledgebase and "how to" articles accordingly, including tips and FAQs.
- We will identify Service Desk agents needing additional training.

2.6.1.5. Describe the approach to resolve problems that impact both County and non-County End-Users (e.g., emergency medical systems).

Our approach to resolving issues that impact both County and non-County users takes into account that the HPES Service Desk plays a crucial role in supporting the County and non-County End-Users.

The Service Desk quickly identifies VIPs and critical systems issues and we page our on-site technical support at the County Administration Center (CAC) and County Operations Center (COC), Rancho Bernardo facility, and AT&T facility on Trade Street to resolve. We empower our deskside/field workers with a full range of capabilities on their mobiles, providing them instant access to EKMS work instructions specific to issues in the field.

Our HPE Service Desk agents provide elevated support when it comes to critical events in the County. Critical or special events include but are not limited to the following classifications:

- County-wide disasters/emergencies. For these events (e.g., fires, floods, power outages), the Office of Emergency Services (OES) is activated and support personnel are required to work with the County to support the end users and the public. The size of these events vary, and Local Assistance Centers (LACs) may be required
- Disasters/emergencies that are small in scope. Response to these events (e.g., focused areas of flooding, building damage) are typically initiated by the Business Group that is impacted. In some cases, a relocation is required to continue to provide service, or an LAC must be stood up. Examples of recent events include the flooding in Ramona, CA, and the roof collapse at the Rosecrans facility.
- Elevated service levels are activated for the Registrar of Voters in support of elections.
- Elevated service levels are activated for Treasurer Tax Collector in support of several public-facing activities conducted by the County.

Each of these events has a documented process in place to ensure that our agents and staff not only understand these requirements but also can route calls appropriately for resolution. Recently, we have added the support of CalFire and the sub stations that they provide across the County. The Service Desk agents have everything they need and are trained to support this effort and are able to distinguish between an emergency event and standard call.

The County provides HPES with a VIP priority matrix and a list of County and non-County VIPs. We have added names and systems to the list and have identified approximately 250 VIPs and mission-critical users, including the following County officials:

- County Board of Supervisors (BOS) and its staff
- Elected officials (e.g., Sheriff of San Diego County, 18 city mayors, and the members of 18 councils) and their designated representatives
- Chief Administrative Officer (CAO) and her direct reports
- Assistant Chief Administrative Officer (ACAO) and staff
- Deputy Chief Administrative Officer (DCAO) and staff
- Department Directors (e.g., Executive Director San Diego County Sheriff's Department).

VIP critical users include representatives of County and non-County mission-critical applications and systems, such as the County's Health and Human Services (HHS) disaster preparedness systems,

emergency medical services (EMS) systems (e.g., San Diego County EMS) and non-County systems (e.g., San Diego Fire and Rescue systems), private and non-private hospitals, and local EMS agencies (LEMSAs).

Calls, emails, or Service Portal notifications from these VIPs and organizations are automatically flagged at the Service Desk for escalated response. The Service Desk agent receiving the notification follows the mission-critical workflow and the Workflow Manager provides oversight to make sure the call is escalated if it cannot be resolved right away.

2.6.1.6. Describe the methodology proposed to ensure and coordinate on-site support to End-Users is not able to resolve Incidents from the Service Desk.

Some Incident tickets cannot be resolved by troubleshooting at the Service Desk level. Using training, experience, and the knowledge of other frameworks as well as the EKMS tool, the Service Desk agent may determine that deskside support is the necessary next step to resolve the ticket. Before escalation, the Service Desk agent reviews the ticket to make sure that all actions taken in diagnosing and troubleshooting have been recorded in the Comments section.

The Service Desk agent notifies the user that the ticket requires a deskside visit for additional troubleshooting. Then the deskside technician coordinates, via Chat or on the mobile phone or email, the visit date and time with the user. The scheduled time, date, and location are updated in the ticket, which is available for lookup on the Service Portal.

Once the deskside technician resolves the issue, the ticket is set to "Resolved," And follows the "Ticket Closure" process described above.

HPES has located our deskside support personnel at the Rancho Bernardo facility and at the CAC and COC. We will station our mobile phone personnel at the AT&T facility on Trade Street.

2.6.1.7. End-User self-service capabilities provided as part of your proposed approach to Service Desk services e.g., reporting, status checking, problem reporting. Include your proposed approach to increasing communications options of End-Users such as Chat functions or self-service.

Our self-service solution provides end users the option of accessing the Service Desk to open a ticket, obtain ticket status, make an SR, check outages, or perform password reset via the Service Portal from multiple platforms, such as mobile phone, desktop, tablet, or Chat, as shown in Figure 41.

Chat. As part of the Service Desk transformation, we will enable users to use Chat with Service Desk agents to request information, report an incident, or request information on SRs. As with other methods of contacting the Service Desk, Chat begins with the standardized ticket workflow and ends with successful resolution. Agents can handle multiple, simultaneous text Chats. The chat tool that will be used comes as a part of the HPSM toolset that is being implemented for the County of San Diego. The End-User will access this chat functionality through the Service Portal so no additional software will be required on the End-Users devices.

Self Service for Incidents/Problems. Similarly, the new self-service ticket capability option enables an End-User to open a non-critical ticket that is automatically submitted to the Service Desk queue for review and action. The user clicks on "Open Ticket" to submit hardware, software, connectivity, printing, phone, and voice issues, as well as general questions. Users are able to track their ticket status without contacting an agent by clicking the "Ticket Status" tile on the portal.

Self Service for Password Reset. As a part of self-service we will implement HPE's Self-Service Password Reset Tool (SSPR tool.) The SSPR tool delivers multiple ways for End-Users to reset their own passwords. This solution removes the requirement for Service Desk intervention where End-Users

have forgotten their passwords and/or locked their account. SSPR is a web browser-based, automated password reset tool that uses dedicated infrastructure, within the County's domain. It also provides a Web-Services based API that allows password resets directly from the Logon Screen. SSPR can also be accessed by visiting the SSPR Web Page from any supported browser on any device, provided it is connected to the County of San Diego's network. Integration with Active Directory will be completed as a part of Transition. Other repositories to be added as requested by the County via Service Request.

Additional Self-Service Features. Our portal capabilities include more features for both self-service and agent assistance:

Figure 41. End-User Self-Service Capabilities from Multiple Platforms

Whether desktop, laptop, tablet, or mobile, County users will have Service Desk self-help capability.

- Knowledgebase search engine capability provides users on their desktop, laptop, or phone "how to" instructions for resolving common problems. Our Knowledgebase content is standard text information that delivers clear, yet engaging, "show me" instructions that walk the user through resolution, click-by-click. It also provides videos for step-by-step problem resolution.
- FAQs based on our review of questions typically asked by users and Tips that enable quick search on a range of information.
- Self-service password reset online tool that allows users to securely reset their own passwords without agent intervention. Users access the secure system by a simple web-based interface, such as a County public-facing website, linked to the portal but implemented separately.
- Dashboard view of the end-to-end County IT environment. Both County management and users are also able to view Rich Site Summary (RSS) feeds, system-wide notifications, alerts, and other important information that impacts the overall IT environment.
- Mobile device "click to call" brings easy dialing options to contact a service

Our approach to introducing the new technologies promotes early County administration and End-User adoption because self-service saves time and improves user productivity. Among our techniques, we will host training sessions for County users to demonstrate portal and self-service capabilities. On deskside visits, our technicians will demonstrate functionality and answer questions. We will distribute tent cards with "how to" instructions on County desks. When asked how long it took for the workforce to proactively use Service Portal self-service functions on one of our recent implementations, the manager's response was "about 24 hours."

2.6.1.8. Your proposed End-User survey process, including the instrument and data analytic capabilities to perform trend analytics. Discuss how survey feedback will be used to improve overall services.

Our review of continuous improvement opportunities has instigated a transition to a more effective customer survey for break/fix tickets, as shown in Section 2.6.1.1, Figure 39. This format has proven its effectiveness on assessing user satisfaction at HP Global Help Desk. The format is designed to make it easy for End-Users to assess in as little as a few seconds the level of their satisfaction with the Service Desk and provide comments if desired. We will consult with the County on the final design of this survey; upon agreement, we plan to distribute the survey after ticket resolution via email or mobile phone. As it is today, the customer survey will be an automated process. The automated dispatch and collection of the survey independent of Service Desk ensures the survey remains intact.

We will provide survey results on the Service Portal each month for the County. The survey identifies the ticket agent and the type of issue that was resolved. HPSM metrics provide the time taken to resolve the issue and the tier level of resolution, including whether we are meeting our 70% first call resolution rate.

Our Service Desk Manager will collect and regularly review the survey data collected; a reporting analyst will identify trends and mentoring and training opportunities.

2.6.1.9. Describe your proposed approach to increasing communications options of End-Users such as chat functions or self-service.

See our response in Section 2.6.1.7.

2.6.1.10. Your proposed approach to continuous measurement of Service Desk performance. Include how measurement results will be used to improve services, how up to date information posted on the Service Portal will be and scripts will be tuned to increase overall first call resolve.

The Service Desk ticket system, phone reports, and customer interactions and surveys will provide the data needed to the Service Portal. These data points will provide the detail that will not only make certain that we are meeting our service levels, but will provide the level of information that we require to continuously improve our services.

The HPSM Service Desk module enables us to standardize the collection of data, collect more categories of data, and provide more accurate data on which we can identify areas that need or demonstrate improvement. For example, dropdown menus with predefined service issues allow us to enumerate a standardized selection of issues and determine their average time to resolution. It can also indicate agents who take longer than the average who may need more training, are working an issue that may require more documentation, or have come across something new that we need to put in place. We will follow ITSM processes in tying data collection and metrics to continuous service improvement.

The Service Desk Manager defines the metrics needed to improve Service Desk customer satisfaction. He will use the HPSM Service Desk's data collection capability. HPSM logic is aligned with ITSM processes, thus allowing us to collect data not only directly tied to the service levels but also more detailed data that will support our strategy for continuous improvement.

Inputs to this step include collecting data against the service levels. HPSM has the capability to collect data automatically, including:

- Baseline data on call waiting times
- Call abandonment rates
- Initial call handle time
- Resolution time in Service Desk by agent
  - Categorization of predefined issues and their resolution time
- Customer Satisfaction Survey ratings and user comments

Service Desk Manager and Workflow Manager will conduct a daily operations status call to review and report metrics and discuss issues that may have emerged overnight or are trending. This call will take place before County standard business hours to ensure we can resolve issues that were raised from the night before. Together they will review data collected on our response and resolution times. They will develop corrective action plans and implementation schedules to improve areas that are lacking or areas where new items need to be put in place. For example, the data may show a particular break/fix script consistently leads to deskside support escalation. They will identify areas where the script is causing a problem and make recommendations to change the script.

HPSM has more than 150 reports that we can use to gather information. The reporting and data that we will be using from this system can be filtered in any way necessary to for us to either provide the information to those requesting it or to isolate the area in which we need to improve or are making an improvement. As an example, the SDM for one of the Business Groups may want to focus on data for their Group. They will be able to set this view up in their dashboard under their profile so they can focus on the data they need. Information from the various reports that are needed to support the business will be provided to the County via the Service Portal and the various meetings that take place (CTO Operations Meeting, Portfolio Review Meetings, etc.). We will also be discussing the reports to be displayed and who needs to view which set of reports as we move through Transition and build out the Service Portal.

Our ITSM-aligned, seven-step process, depicted in Figure 42, provides a solid foundation for capture and reporting of data to support analysis that we can use to identify opportunities for continuous improvement.

Figure 42. Seven-Step Process for Measuring Performance to Support Continuous Improvement

We follow rigorous ITSM processes using metrics to guide our service improvement activities for the County.

Comparing this data against measurable targets helps us identify the steps to improve an aspect of the operation. Table 24 describes relevant Continuous Service Improvement (CSI) activities, such as service level reporting and management processes, that we have tied to the Seven-Step Process.

Table 24. Continuous Service Improvement Service Desk Approach for the County.

CSI ACTIVITIES	HPES CSI APPROACH TO SERVICE DESK
Steps 1, 2, 3, 4 Performance Metrics	We will capture a performance metrics and capture the same metrics every month thereafter for comparison. HPES will display our metrics on the Service Portal metrics dashboard in a meaningful, easy-to-use format for access by our agents and the County. These metrics will come from HPSM and the Avaya Call Manager system.
Step 3 Customer Satisfaction Surveys and Assessment	In combination with the performance metrics that will be using in steps 1 to 4, we will leverage HPSM Service Desk to collect customer feedback using customer satisfaction surveys. We will regularly review customer satisfaction surveys and follow up on any negative surveys. This allows a feedback loop into the process for improvement as well as follow-up communication to the customer.
Step 5 Identifying Opportunities for Improvement	Our Service Desk Manager, working with our Work Shift Manager and agent leads, will use a real-time portal view of our Service Desk performance metrics (e.g., call waiting time, call abandonment, Service Desk time to resolution, volume of tickets escalated to different resolver groups), data analysis, and lessons learned to identify improvement opportunities for our Service Desk team of agents.
Step 6 Daily Agent Meetings Dedicated to Service Improvement	The Service Desk Manager, Work Shift Manager, and Service Desk agents will meet daily to review areas that need improvement and brainstorm ways to improve performance. For example, should metrics show that Service Desk phone handle time has increased with the use of the script for break/fix, we will work together to see what phraseology is causing the problem and correct it.
Step 7 Corrective Action Development and Implementation	For serious quality issues, we will develop a Corrective Action Plan (CAP) with support from the accounts QA personnel that includes a timeline for implementation. Following implementation, we will gather metrics specific to the issue to measure progress.

We provide a sample of our continuous service improvement activities tied to our seven-step process.

2.6.1.11. Your proposed approach and design for the Service Portal. Include how it will be maintained and supported with timely, accurate and complete content across all Service Framework.

We will use HPE Service Manager (HPSM) software at the core of our ITSM Service Desk. HPSM includes our integrated Service Portal solution for providing a closed-loop incident process and user self-service Incident resolution, SR creation, and information search. HPSM together with the Service Portal provide multiple dashboards easily accessible by County users and HPES management, and Service Desk agents.

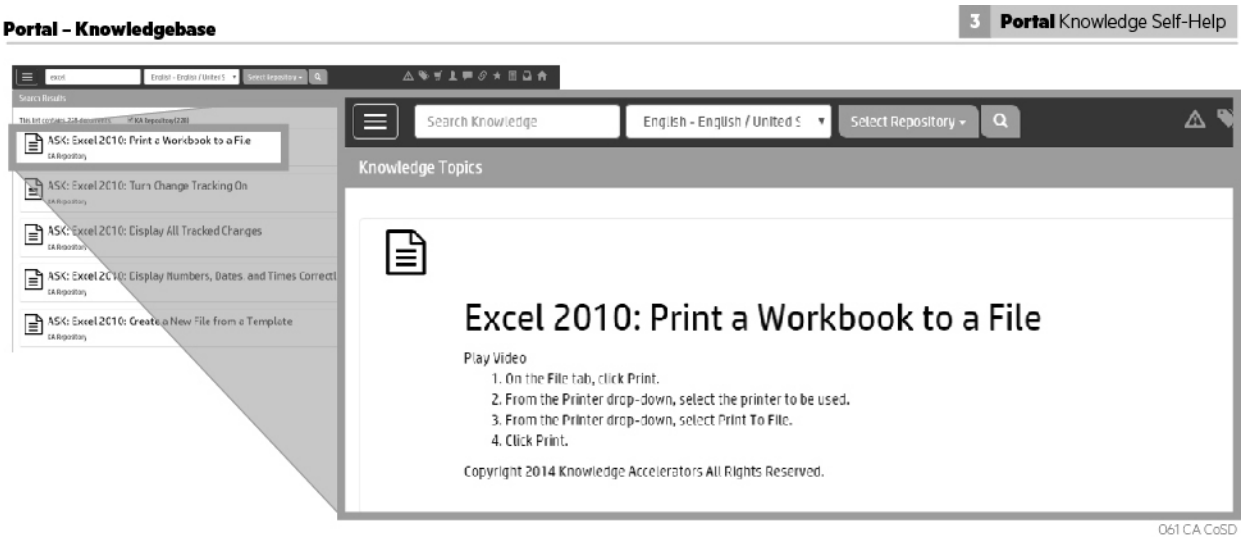
We look forward to working with County stakeholders in developing the branding, look, and feel of the portal as well as expectations of functionality.

Key components of the Service Portal we are proposing include:

- Access from both the Internet and the County Intranet
- Support for key processes, including incident, problem, change, SR (interaction), self-service, and service asset and configuration management
- Single sign on (SSO) integration and predefined roles and rules

- Improved, standardized screen layout with "smart indicators" to flag related information
- Rich cross-process functionality via a range of wizards
- Management reports, service-level reports, all required County deliverables
- Service Desk-specific components include:
  - Service levels built in with data analytic capability that generates reports such as ticket volume and response times
  - Self-service access to the Service Desk to open a ticket, access the Service Catalog, make an SR (through the SR management tool discussed in Section 2.6.1.12), access ticket and SR status, see announcements including number of outages
  - FAQs, tips, training, and self-service password reset capability
  - County-dedicated EKMS for technical support teams that includes documentation and flowcharts for processes, procedures, RCAs, and high-level work around instructions across the frameworks
  - A self-service indexed Knowledgebase developed specifically for access by all end users, upon County approval, to help them obtain the best answers in real time to their request for information and resolve low-complexity problems, as shown in the "how to" instructions in Figure 43.

Figure 43. Self-Service Instructions



Our Knowledgebase for users will enable them to make easy fixes and find information quickly.

2.6.1.12. Your proposed approach to Service Request Management Services. Include how it will be maintained to include current content from across all Service Frameworks.

Our solution is to provide Service Desk agent assistance for fulfilling SRs and to enable users to create their own SRs on the electronic processes of the Service Portal's self-service capability. Our Service Portal will use HPSM and myRequests, the current application for SRs and ticketing, that will provide the entry point for other tools such as SharePoint. After the Transition phase is complete, our plan is to migrate myRequests to HPSM's more advanced SR functionality. We will initiate and execute this project and its design at a time expedient to the County's priorities.

We will work with County framework administrators to capture and document all SR-related content and maintain it in a rules-based database within the SR Management tool. We also propose to develop a Service Portal version of the OIC Service Catalog.

Service Desk Agent SR Assistance. Our Service Desk agents currently assist users with submitting SRs for items such as installs, moves, additions, and removals (IMAR) or changes to the workplace environment.

Service Desk will continue to provide this service, by creating records on SR forms, copying an existing record, or applying a predefined template that prefills specific fields using electronic processes:

- The user makes the SR to the Service Desk by phone, email, fax, or the Service Portal.
- The Service Desk agent determines if the SR is a request or an Incident and follows a closed loop process
  - If the request is an Incident, it is handled as discussed in Section 2.6.1.
  - If the request is an IMAR, the agent will refer to the appropriate documentation to make certain that the request is routed properly to the appropriate framework. Details of this process are provided in Section 2.7 End User Services Framework - IMAR
- The Service Desk agent categorizes the request and assigns a priority level.
- The Service Desk checks the Service Catalog, which is based on the OIC Service Catalog, to determine if the SR needs approval and, if so, the level of approval required.
- If a request is approved, the Service Desk agent escalates it as appropriate, and updates the user upon request.

Service Requests by Self-Service. Once the Service Portal is implemented, the user will be able to make SRs on user-friendly SR forms that are routed to the Service Desk ticket screen (in accordance with the approvals granted by the County). A Service Desk agent will be assigned the SR that arrives from the portal and will review it and follow predefined steps in a workflow, including classification, fulfillment, and validation.

Service Portal Service Catalog. We propose developing a version of the OIC Service Catalog suitable for Service Portal self-service. We envision the portal's version of the Service Catalog to be accessible to all end users for making Service Catalog-based SRs. The SRs will display the approval process required to the user before being routed to the Service Desk. A Service Portal version of the Service Catalog will provide the following benefits:

- Reduces Service Desk's workload by providing self-service capabilities for Service Catalog requests that flag approvals that are required
- Ensures all self-service SRs are routed to Service Desk for review
- Provides a single, guided, questionnaire-style user interface for requesting support for catalog and non-catalog items
- Provides tablet and mobile user support.

Figure 44 provides an example of self-service SR request for a new tablet.

Figure 44. Self-Service Request for Hardware

County users will see flags for approvals required when they select an item from the Service Catalog.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Service Desk Services Framework – Executive Summary

We summarize our benefits to the County in Table 25.

Table 25. HPES Solution Benefits to the County.

SERVICE DESK SOLUTION FEATURES	BENEFITS TO THE COUNTY
HPES Service Desk agents have been supporting the County since 2006	Service Desk agents are familiar with County scripts, processes, escalation procedures and VIPs.
Knowledge database expansion will be built upon the solid foundation of existing County scripts	Current knowledge database is well-known to Service Desk agents. Training needs will be minimized: required for new processes/functions.
World-class HP Service Manager system for ticket automation proven successful on large and small user base contracts	Mitigates risk to the County by implementing required technology that has proven successful on similar-sized engagements Brings world-class automation based on HPE's use of best practices

SERVICE DESK SOLUTION FEATURES	BENEFITS TO THE COUNTY
Customizable Service Portal with self-service capability	Builds County priorities into the screen and functional design before implementation
Multiple platforms for user access	Enables users from any location to access all features of the Service Portal (chat, ticketing, reporting, etc.) — home, field, in the office, or in a hospital or emergency vehicle—to access help from their mobile phones, tablets, desktops, or laptops
Service Desk Manager with management experience	Provides County leads with a collaborator they have already worked with and no learning curve
Innovative agent training and orientation program that makes "Doing Business with the County" training mandatory for current and new agents Increased Service Desk management personnel at Service Desk locations Training analyst focused on improving agent-end user interaction	Provides the County Service Desk agents with deeper understanding of the pressure users bear when IT issues remain unresolved or SRs are not fulfilled in a timely manner Provides County with agents trained in Service Desk industry best practices

2.7 End-User Services Framework

Executive Overview. Just as County employees represent a critical touchpoint to the citizens of the County, End-User Services represents a critical touchpoint to County employees. As the incumbent, HPES is successfully delivering this End-User Services framework to the County. Most of our team members are also residents and are directly impacted by the end results. We take great pride in providing excellent customer service, quick resolution of customer problems, and assistance that contributes to the success of the County's business for the public they serve. Based on our current successful services, we anticipate a low-risk transition of this framework to the new contract. Upon transition, HPES will implement exciting changes such as expanded mobile device management and Skype for Business (SfB).

Current Environment. HPES currently supports more than 250 sites and 16,000+ users with more than 15,000 desktops and laptops, and 1,000 printers (networked and attached). We also support mobility, with more 500 tablets and Surface Pro devices, and 3,600 smartphones, plus tablets ruggedized for field work with citizens. We are meeting an increased demand for mobility, especially Bring Your Own Device (BYOD). Install, move, and add, remove (IMAR) volumes are large, with 650 site support IMARs per month. The desktop environment is predominantly MS Windows, and users have flexible storage options including local, remote, private, and shared—all are appropriately secured.

Summary of Framework Solution. We will retain the same centralized management and control that is in place in the County today. We will use ITIL-based procedures including processes and procedures that we have developed, put in place, and improved during the past 5 years. Our service is supported by the HPE Service Center tool, which will migrate to HPE Service Manager (SM) in 2016. End-user support services will be implemented within the IT Service Management (ITSM) framework delivery model. Also, we will support this environment using specialized tools such as Microsoft System Center Configuration Manager (SCCM), LogMeIn Rescue, AirWatch, MS Office Configuration Analyzer Tool (OffCAT), HPE Diagnostic Toolset, Endpoint Encryption, Endpoint Protection, and WebSense.

Hector Vaquedano will lead the expanded End-User Services organization. Other existing personnel, solutions, methodologies, and procedures will stay in place, making the contract transition seamless to County users. During transition, we will migrate your users from traditional, data center-hosted MS-Exchange email to Office 365 Online, in the cloud. AT&T will continue to be our partner for Mobile Device Management (MDM) via AirWatch and network services.

HPES is committed to keeping End-User Services and technologies operating at the required performance levels and will provide services to support these technologies within the required timeframes. We will continue to provide excellent service with minimal to no disruption to the County and the public. Our goal is to sustain and build on the relationships and the performance we have today. We understand that collaboration with the County is key to our success and we will continue to earn the privilege to do business with the County.

Desktop Computing Services (Sched 4.3, Section 4.5)

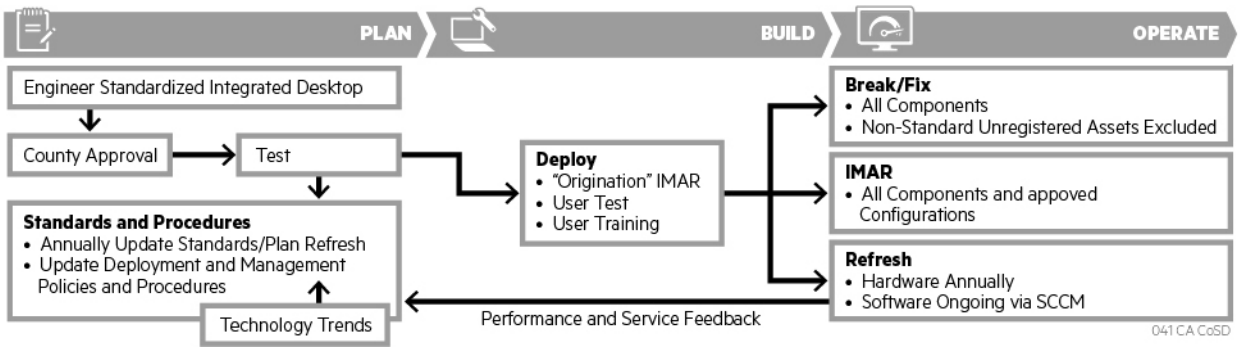
- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES' Desktop Computing Services framework solution integrates all required components of End-User Services, interfacing components (such as Service Desk) and cross-functional components (such as Asset Management). Based on the engineering support and services we provide, any technological complexity to plan, build, operate desktop configurations and services should be transparent to County users and their customers, the citizens. The Desktop Computing Services component is central to all elements of End-User Services. Figure 45 illustrates our integrated framework, which also maps all elements of the statement of work to demonstrate the completeness of our solution, and shows a reference point for the

scope and integration of the other framework and cross-functional components and tools, such as Service Manager.

Historically a stable, reliable, well-performing framework component, HPES will continue to use the existing framework methods throughout the transition for a smooth and reliable process. The framework is driven by the "plan, build, operate" concept, as illustrated in Figure 45. Additional detail is in the methodology and key processes section below.

Figure 45. Desktop Computing Services Activities across the Plan, Build, Operate Lifecycle



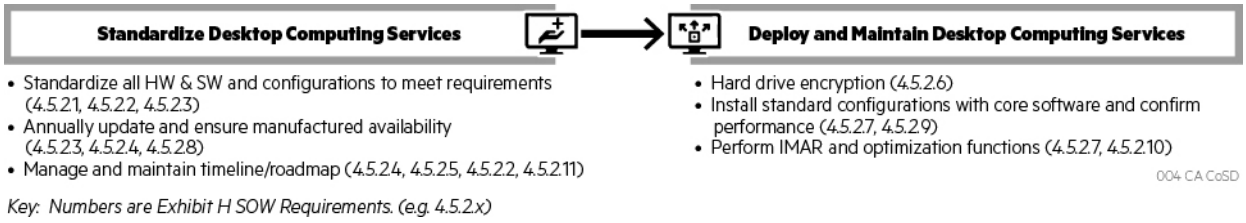
We manage the desktop services and architecture as an integrated solution across the Plan, Build, and Operate life cycle structure.

Rationale for Choosing This Solution

Our Desktop Computing Services solution builds on existing performance, reliability, relationships, and trust that HPES has with the County today. We regularly receive positive feedback and customer satisfaction scores and meet all service levels; our internal HPES teams (engineering and testing) will continue to make improvements in collaboration with the County going forward. This solution will continue to enhance the optimal customer care required to provide a solid, low- risk approach for contract transition while providing the foundation for future enhancements to End-User Services as County-approved transformation activities.

This solution will provide standardization as a key component to optimizing service (see Figure 46). The bulk of our efforts will focus on enhancing our services to the County— best accomplished by standardizing a set of technologies that recognize the diversity of the employee base and also derive support, cost, and efficiency benefits. We also recognize the need for flexibility to provide nonstandard solutions or technology where needed.

Figure 46. Desktop Computing Services Solution



Standardization is key to optimizing service.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Facility Approach. Desktop Computing Services will continue to be provided by an HPES services team located centrally at our Rancho Bernardo facility. Additionally, we will continue to have embedded support technicians at the COC and CAC.

- 1 employee will continue to reside at the COC
- 2 employees will continue to reside at the CAC

As service issues require in-person support, HPES deploys technicians from our regionalized end-user support team. Most site technicians reside and will continue to reside at HPES' Rancho Bernardo facility. The technicians use this as their home base, traveling to any of the County sites with the equipment and tools required.

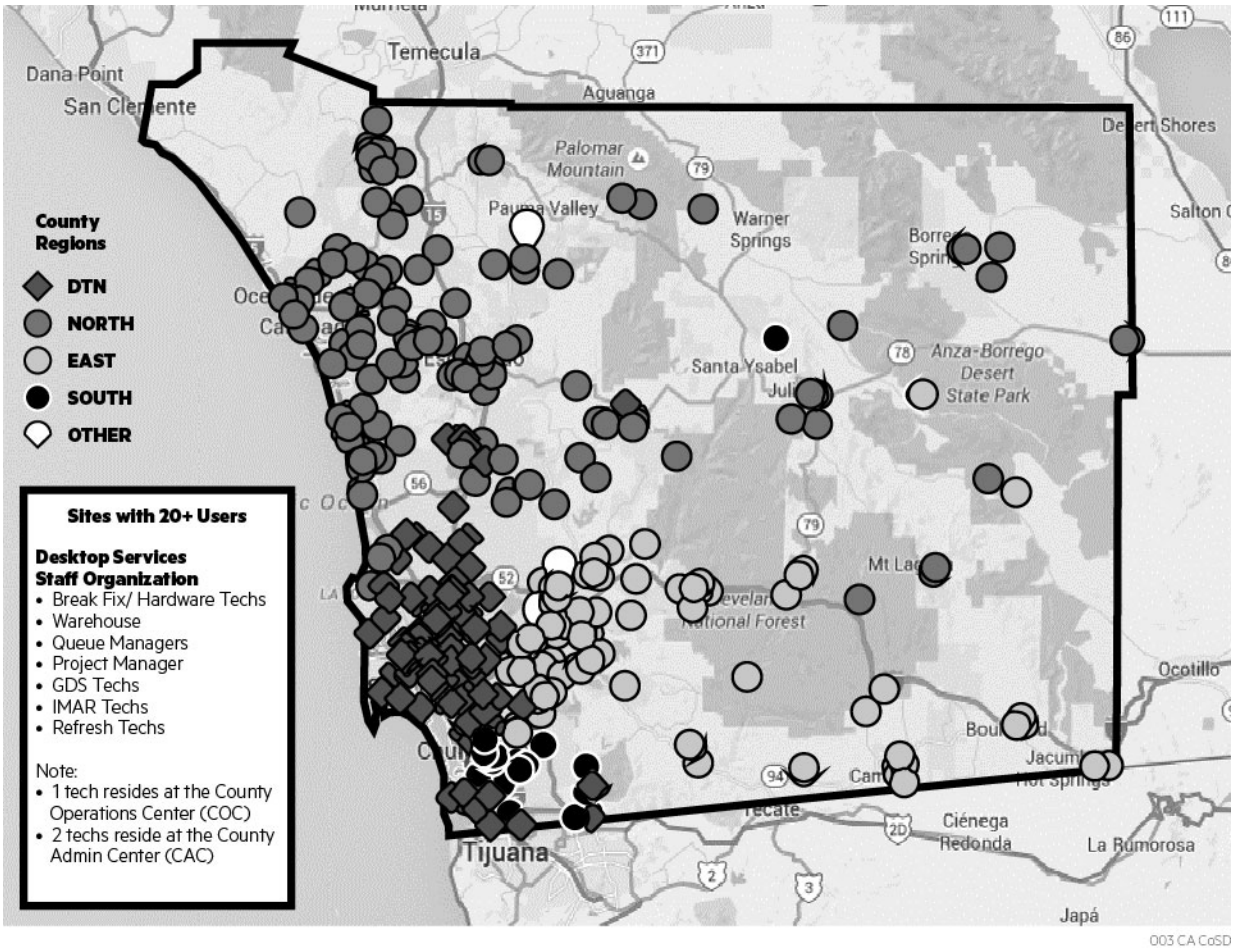
We staff the core hours of Monday through Friday 6:00 a.m. to 6:00 p.m. with a full shift. Non-core hours are staffed at levels sufficient to provide necessary service as required over the weekends, on holidays, and after the business day. Our support service levels are available 24x7x365. Online ticket creation is available with the Service Desk 24x7 via the Service Portal, phone call, or chat, so even non-urgent service tickets can be logged anytime.

Service Management. To serve all the sites that do not have dedicated onsite support, HPES has a functionally organized technical support team. This team travels in a fleet of vehicles, each of which is provisioned with spare parts and "hot swap" spares to provide "first-touch" issue resolution where possible. After assessing the problem, our technicians have the necessary troubleshooting skills and are empowered to do the right thing—up to and including a "hot swap" of the equipment—to get user service restored quickly. We then take the faulty equipment back to the warehouse for more extended diagnostics and repair while the user continues to perform their job on the new equipment.

Service Scheduling. Service technicians provide numerous types of service, including break/fix ticket requests, IMAR actions, or software refresh. Hardware and core software configuration refresh actions are planned for implementation throughout the year. IMARs are also planned in advance and are non-emergency. For event-driven break/fix service, technicians are deployed by the queue manager based on the functional content of the ticket and the user's location. Figure 47 shows the geographic coverage of end-user support and summarizes the functional organization of End-User Services.

Emergency Management. In the event of a disaster or emergency, the Desktop Computing Services team, along with the framework teams, provides immediate services to the County of San Diego. These events result from floods, fires, large-scale power outages, or other disasters—and we have provided support for these types of events many times over the past 5 years. The Office of Emergency Services (OES) within the County can activate or an individual business group will reach out for assistance and support. When the OES is activated, the service delivery manager (SDM) on call, along with the Infrastructure Operations Manager, is immediately dispatched to the County location with a desktop technician to provide the first shift of support. We have built a robust rotation of management and technicians that will remain on site with County staff and other entities that are brought in to support the effort.

Figure 47. Functional and Geographic Organization of Service Staff



Service Personnel are organized and deployed to be most responsive.

Typically when these events occur, members of the public are affected and need support from the County to obtain housing and food, file insurance claims, and so forth. To support these communities, we work with the County to stand up Local Assistance Centers (LACs) strategically placed where the event has occurred. HPES, along with AT&T, provides all the equipment, connectivity, and onsite staff to provide onsite County employees with everything they require. If the OES is not activated and a request comes in from a business group to provide support for a disaster, we implement the same process and provide the same support. Events that we have supported include the following:

- 2011 – Large-scale power outage impacting all of San Diego
- 2014 – Multiple fires impacting several areas in San Diego
- 2015 – Floods in Ramona
- 2015 – Rain in San Diego causing a roof to collapse at a County site

As residents of the County of San Diego ourselves, we understand the need to not only support our customer but the public as well. While we hope that these are rare occurrences, we keep the necessary measures in place to make sure that we can mobilize quickly and provide support as soon as it is needed.

Service Technician Skill Profile. The minimum skills and experience required for all technicians are as follows:

- Desktop OS (Windows 7, Windows 8.1), with mandatory Windows 10 training for all techs underway
- Basic level server hardware replacement skills
- Customer service skills
- Basic data backup skills
- Minimum 2-year remote and onsite troubleshooting experience
- Attention to detail
- Deskside user and technical communication skills

All technicians have the same base skills and are cross-trained so that, in periods of surge, we can flex our normal operational processes to meet the service demand. This human resource strategy enables us to provide constant, consistent surge or emergency service to all IT users throughout the County.

Many technicians exceed the minimum requirements for the position. Across the organization, we have specialists in the various technologies—MDM, Network Printer, Communications—and functions—IMAR, Technical Refresh, Break/Fix—to perform most efficiently and provide reach back expertise to everyone.

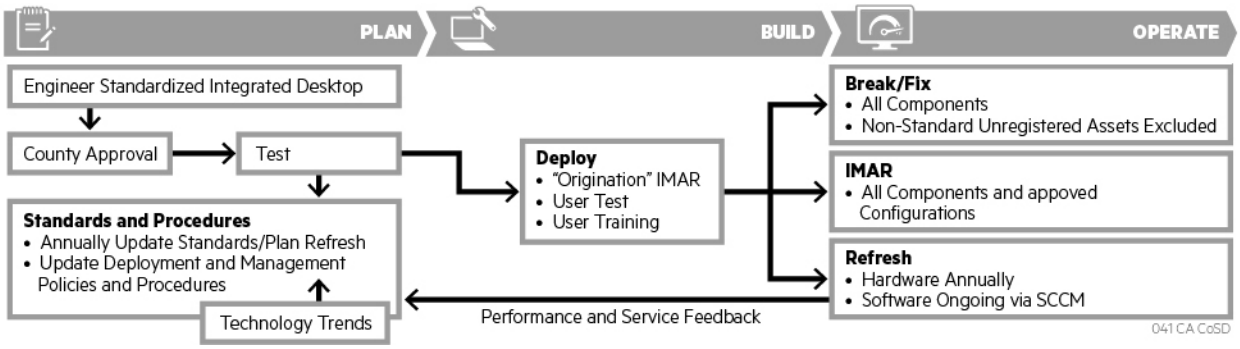
In addition, we provide communications to our service technicians to keep them up to date on the County's mission via all-hands meetings, webinars, leadership briefings, weekly/monthly newsletters, knowledge shares, and other County specific activities.

Finally, our service technicians stay aware of HPES and industry state-of-the-art and best practices via newsletters, webinars, the internal HPES portal, team meetings, and so forth, for information about the latest technology, and for continuing education, to provide exceptional customer service.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Figure 48 serves as a roadmap for our Desktop Services Methodology.

Figure 48. Desktop Services Methodology



The **Plan Phase** includes engineering, testing, establishing standards for desktop hardware and software, and obtaining applications approvals. These standard core configurations are documented in Reports 43 and 44. The standard desktop configurations are re-assessed and updated annually with County review and approval. During this annual review, the technology may or may not change; for example, Internet browsers are a relatively consistent and stable component of the desktop configuration. A significant amount of coordination, approval, engineering work, and testing is required to do a browser update. Update decisions depend on complexity, user benefit, technical necessity, County approvals, and so forth. HPES will continue to bring full transparency and engineering rigor and review into the annual update process. The Optional Items Catalog (OIC) includes non-standard items that the user may still require. In addition to supporting the current field equipment, the standards engineering function also includes forward-looking work with vendors and the greater technology community to anticipate and plan for

future incremental and transformative configurations. These are documented in the timeline/roadmap documentation and briefing to the County annually.

The Desktop Engineering organization maintains, updates, tests, and annually releases the standard hardware and software configurations. For example, there may be updates during the calendar year to account for a product no longer being available from the vendor. Desktop Engineering will work with Enterprise Architecture to integrate into the environment, and provide cross-training to the Operations team. This group coordinates engineering and testing prior to deployment to address and eliminate issues such as older drivers and network interface card (NIC) mismatches.

We conduct a weekly Infrastructure Project meeting to discuss the current status of ongoing infrastructure-related projects in the environment. Enterprise Architecture meetings review, for example, new technologies, changes to the desktop hardware and software standard and , technical requirements for a project. These meetings help us to collaborate with the County on all important ongoing and new engineering requirements and issues.

Currently, hardware standards are published in the annual "Report 44" to the County.

The **Build Phase** includes the full set of activities to assemble, deploy, and test each individual standardized unit (with approved options); these include desktops, laptops, tablets, printers, and other network resources in a standardized MS-Windows based environment. The following bullets describe our process:

- Upon receipt of the hardware, we tag it and kit what would go with it and have it ready for imaging when needed.
- The machine gets pulled from the warehouse, and prepared to be imaged based on the configuration requested.
- Once the image/applications are completed, validated, and tested, we put the equipment in the warehouse, where it is kitted with all of the accessories, and the device is ready for delivery.
- Service ticket documentation or communication from the refresh the project manager then tells the technician where and to whom to deliver the hardware.

Desktop Engineering creates a custom enterprise operating system (OS) image for the County, which comprises the MS Windows operating system (Windows 7 and Windows 8.1 are current standards) and device drivers. Device drivers are for the network interface card (NIC) of the laptop/workstation, printer drivers, etc. This custom OS is made available to the imaging technician who handles imaging for refresh, IMAR, break/fix. During the business day, we have staff onsite in Rancho Bernardo in the imaging room that can complete hot swap devices for loaners as needed, and copies of these images are provided to the technicians in the field for onsite re-imaging.

The **Operate Phase** includes the maintenance, operations, refresh, IMAR, break/fix, and everything else to support daily operations for the user. Operations and support activities cut across the frameworks and integrate User Service functions from the Service Desk, such as ticketing and remote support; service management functions such as asset management, configuration management, and process improvement; and other components of the End-User Services framework. Cross-Functional Services are described in detail in Section 2.5. Service Desk is described in detail in Section 2.6. Specific "operate" functions are described in the appropriate component sections. Generally, the process is as follows:

- Ticket requesting action is received, logged, and dispatched to a technician.
- Technician performs the required action to resolve the user's issue in accordance with documented procedures and services standards.
- Functional operation of the hardware and/or software is validated by the technician before permission is obtained from the end user to close the ticket

- User satisfaction is confirmed verbally and via the Customer Service Survey sent out at the closure of the ticket.
- Asset management database is updated, if required
- The ticket is closed.

Hardware and software not in the standard configurations—BYOD smartphones, standalone printers, etc.—are supported as non-standard items. While these items are not standard, we do understand the importance behind what each County employee does and the fact they cannot be without what they need to perform their business functions. We have processes in place today to support requests for service on these items on an as-requested basis. Two examples in place today are as follows:

- The Nondiscretionary work request (NDWR) from HHSA to repair the CMIPS printers procured by the County
- The NDWR from HHSA to support the 600+ Kodak Scanners required to support the CalWIN Electronic Records Management System (CERMS) application

The Desktop Computing Services component—the first of the components to be discussed—is used to integrate all components of the desktop configurations: hardware, software, applications, network print, communications and, MDM. When we discuss the integrated configuration or integrated desktop, we are referring to the integrated functionality of all components. Some of the components are discussed in detail in subsequent sections, in support of RFP requirements structure.

Scheduling

For the annual refresh requirements and schedule, we attempt to complete all the equipment at a given location before moving to the next site. This approach minimizes disruption to the users at the active site. Communications go out at multiple points for each device to prepare the users and avoid as much disruption as possible on the day of refresh. A target schedule is provided on an annual basis to the identified points of contact (POCs) to review and make edits as needed. We are flexible and work with the County's IT coordinators directly, along with the CTO point of contact, so that if changes need to be made to locations and dates, we accommodate them to prevent disruption. We have a dedicated project manager assigned to the refresh activities of the end-user devices to provide solid communication, consistency, accuracy, and delivery of services in this space. The project manager is also responsible for the overall status of the project plan created annually for each refresh cycle and reports on that weekly in the Infrastructure Project meeting.

Refresh.

Technical refresh is performed on a rolling basis throughout the year based on equipment type, install date, and refresh timelines, as shown in Table 26, which lists Technical refresh frequency by device type. There is a 6-month refresh availability window that starts 6 months before the scheduled refresh date and a 2 month grace period after each refresh date. We take these into account during refresh planning and optimization. HPES is flexible in its planning with the County, so we may exceed the 6-month early refresh window based on County requirements.

Table 26. Technical Refresh Frequency

EQUIPMENT TYPE	TECH REFRESH CYCLE
Standard Desktop	4 years
Ultra-Portable Laptop	3 years
Engineering Workstations	4 years

EQUIPMENT TYPE	TECH REFRESH CYCLE
Engineering Laptops	3 years
Ruggedized Laptops	3 years
Ruggedized Tablets	3 years
Convertible Tablets	3 years
Printers	4 years

In addition, the County may request an early refresh of a desktop computing asset through the IMAR process at any time out of normal refresh cycle. If the device is not in the current refresh schedule or the request date is greater than 6 months earlier than the normal cycle refresh date, the department will be charged a pre-defined rate per month based on device type.

Desktop Computing Services has a team of refresh technicians who specialize in performing refreshes. The technical refresh process is as follows:

- At the beginning of the calendar year, a draft schedule is communicated to the County
- We work with the County to around any County business events. We then finalize the schedule with the County coordinator.
- Prior to performing planned work at a site, we communicate with the coordinator to validate planned activity is still acceptable.
- A review every device is completed 3 to 4 weeks in advance of the actual refresh to identify custom configurations, applications, standalone hardware requirements, replacement model, extra tray requirements, and so forth.
- Equipment, including software configurations, is prepared to the extent possible at the warehouse prior to delivery to the user based on the information from the pre-field form. This includes hardware configuration, any hardware default settings, basic software imaging, and standard software configurations.
- Testing is performed.
- Communications are sent to End-Users and POCs during all required steps of this process to make certain that nothing is missed.

At the user site, we back up configurations from the machine that is going to be replaced; note that the County's policy states that no user data should be stored on the device. Users are notified during pre-communication to move data off the devices and onto shared data locations. The technician will assist with any data that resides on the device that is related to applications and up to 30 minutes of "other" data transfer as a part of the refresh scope of work. The following actions are performed by the refresh technician at the user's site:

- Disconnect existing hardware, noting and/or tagging anything user- or site-specific, unique or non-standard.
- Install new hardware in the standard configuration, noting and addressing anything user-specific.
- Restore user configurations onto the new equipment; re-establish network access and network configurations.
- Perform functional tests to demonstrate to the user that the refresh was successful. Troubleshoot any issues.
- Make the user aware of any new features/functions of the new configuration and equipment. Point the user to relevant frequently asked questions (FAQs) or training, if needed.
- Notify the refresh project manager that the refresh is complete.

- The refresh project manager updates the database and reporting measures as activities are confirmed completed by the technicians.
- Notify the Service Desk that the ticket is complete.

In addition to desktop hardware refresh, there is an ongoing stream of major and minor software updates. These updates are managed by SCCM and are usually automatic and transparent to the user. Software Refresh is described in more detail in the next component section.

Break / Fix / Hardware Technical Support

Break/fix services are event driven and triggered by a service ticket. Technicians manage service on the integrated desktop configuration, not just the hardware. Currently, approximately half of all support requests are resolved without the need for a deskside visit; we meet or exceed service level requirements in this area.

Queue Management. Within Desktop Services, the queue manager assigns tickets to technicians. This function is performed via a process supported by MS Office tools for scheduling. Technicians are assigned in an optimal manner, based on a combination of technical requirements, urgency of the ticket, geography of the ticket, and the technical complexity of the problem. For VIP service, we strive to assign a familiar and experienced technician the VIP knows and trusts. When a problem requires desk-side support, we use the following methodology:

- Ticket forwarded from Service Desk to queue manager
- Queue manager determines whom to assign the ticket to
- Ticket is assigned to a technician, and the technician is notified of the ticket assignment
- Technician travels to user and performs the appropriate diagnostic protocol for the identified problem

The nature of troubleshooting is too voluminous to specify all break/fix scenarios here. However, to diagnose the issue, generally technicians will use tools such as HP Diagnostics Toolset, LogMeIn Rescue, SCCM, Active Directory (AD), MS OffCAT, AirWatch, and others, depending on the nature of the problem. Most problems can be resolved with fairly straightforward troubleshooting and repair. Technicians have additional options available for more complex problems:

- Correct the problem at the deskside using break/fix troubleshooting procedures for the specific problem
- Get peer level technical specialist support to assist with problem resolution
- Escalate to a SME as appropriate
- Hot swap to a loaner
- Hot swap to a spare

Technicians will select the right method to get the user back in service as quickly as possible while still resolving the root-cause technical issue. The technician tests and demonstrates to the user that the problem is fixed.

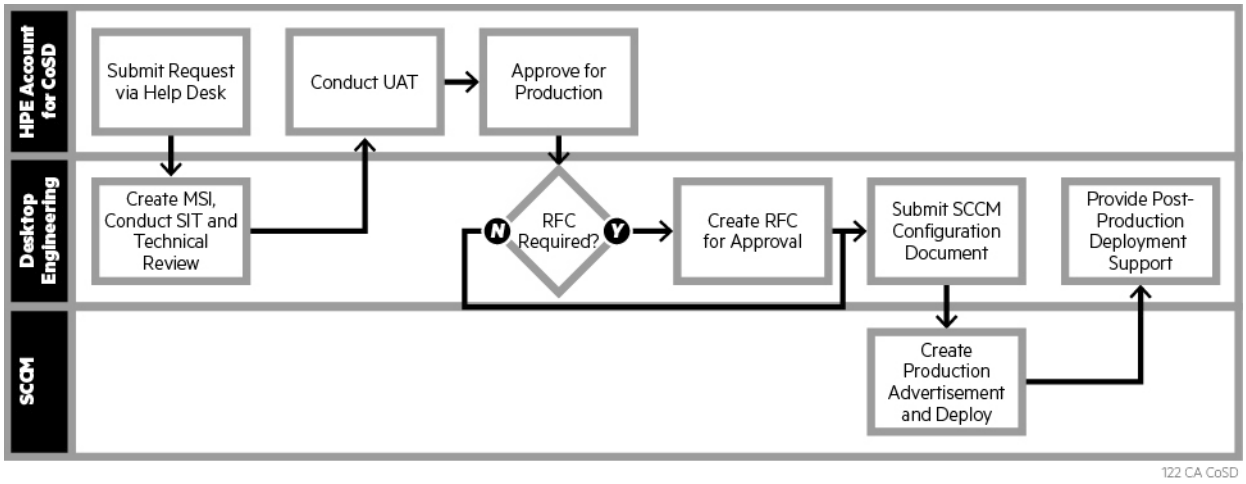
- The technician performs the foundational set of system and end-user testing, which is a series of standard tests.
- Technician logs the fix, updates the asset inventory (if necessary).
- Upon completion of the service, the technician moves on to work their next ticket

IMAR.

IMAR requests are typically triggered by non-urgent events. An IMAR could be an "origination IMAR" for a first-time install; it could be a simple or complex configuration add or modification request; it could be a move request for either a single user or a suite of offices; or it could be a removal event associated with technical refresh and equipment upgrade. Any IMAR request that comes in with more than 25 items

is considered a project and is assigned within the End-User Service group to the project coordinator to manage and complete as required. The IMAR process flow, illustrated in Figure 49, is the same as for all other types of requests.

Figure 49. IMAR Process



An efficient, standard IMAR process is essential for the volume of changes at the County.

Keeping asset data up to date is always important; this is especially applicable to IMARs. HPE Asset Manager tracks all modifications to an asset record that are the result of moves (locations, users, and so on), adds (adding components), or changes (any other changes to the asset record). Modifications are tracked by field. If a field value is changed, HPE Asset Manager captures the name of the person making the change, the date of the change, and the name of the field that has been changed as well as the previous field value.

Moves, adds, or changes to assets can also be discovered or confirmed through auto-discovery, using the DDMi (Discovery and Dependency Mapping Inventory) tool for consistency. For example, if the IMAR project involves removal of software from a computer asset, the auto-discovery tool may be used to confirm that the software has been removed. HPES also provides tools to automate software-related IMAR activities, including policy-based software management. An IMAR action can be for a complete desktop, laptop, or other device configuration or just a component. Overall, the IMAR process is as follows:

- Receive an IMAR ticket
- Travel to the site of the equipment/bring equipment to the site location for install
- If the equipment is onsite, complete the identification and validation of this equipment to make sure inventory numbers match the tickets and asset database
- Back up all relevant user data and configurations and other environmental settings if required
- Make the appropriate IMAR action as indicated in the request:
  - **Install.** The "origination IMAR" is a special case of installation. For the first installation, the equipment is new, newly refurbished, or wiped to a new configuration. Where we are able, new configurations of equipment can be prepared in the warehouse with hardware configuration, the standard software image installed, and any user optional items installed. This preparation work will ease the installation process at the user's desk. Then configuration to the user's environment—for example, preferences, network connectivity and printer connectivity—is completed.
  - **Move.** A move is similar to a remove and install, except that software installation does not need to be performed. For a move, the technician will note the user's connections and configurations,

power down the old equipment, minimize its disassembly but do enough disassembly to safely move the equipment, and then physically move the equipment to the new location. Once at the new location, the technician performs the necessary installation steps completing with reconfiguration of user-specific and site-specific parameters.

- **Add.** An add is typically for a new piece of hardware or software. Procedurally, an add can be thought of as an install, and follows similar steps.
- **Remove.** Complete removal of equipment can happen when a user leaves the County or when the equipment they are using is refreshed. Upon removal, the technician will shut down the equipment, making necessary logical and physical disconnections and take the equipment away. Removed equipment goes through the warehouse for asset management and proper disposal. Hardware at end of life is so noted in the asset management database and is donated to San Diego Futures Foundation (SDFF). Removals of software include an action to make certain that any active licenses that were originally obtained are returned to the licensing pool for reuse.

IMAR Testing. In all actions that result in retained or upgraded equipment, the technician validates via deskside testing that the user functionality is correct and user configurations are created and/or retained as appropriate. This deskside test process is similar to that described in break/fix.

Continuous Improvement. Today we provide Desktop Computing Services with continual improvement in mind. We always seek to implement new solutions and processes that will help us to provide better services going forward. This mindset continues into the End-User Services space in this proposal, using the ITIL Continual Service Improvement (CSI) process. Putting this formalized methodology in place will sharpen our focus on improving the quality of the services or improving their efficiency for the County.

- Using the Deming PDCA (Plan/Do/Check/Act) (see Figure 50), we will on a continuing basis seek to improve End-User Services by finding improvement areas, planning remediation's and implementing them, and measuring the change in our quality metrics.
- End-User Services is a data-bound group. Guiding our quality goals are the service levels measuring our performance along with the Customer Satisfaction Survey data provided. The service levels and surveys are leading indicators of quality, but we also have all the data and analytics about the installed configurations and break/fix trends such as types of tickets, hardware configurations involved, system performance to ensure maximum optimization of the desktop environment, the nature of problems, time to repair metrics. These are the leading indicators of quality.
- We will analyze these indicators to determine if we need to embark on a Service Improvement Plan to improve our quality. These efforts are tracked, and the team recommends improvements. After putting them in place, we will then monitor closely both the incident and problem trends and their impact on our service level performance.

Figure 50. Continuous Improvement

Continuous Service Improvement facilitated by the Deming Plan/ Do/ Check/ Act cycle.

For example, if our metrics find customers are dissatisfied with how long it takes for a service technician to arrive deskside, we determine why and implement a solution to prevent the issue from reoccurring.

During the cross-functional transition, we will implement Microsoft SQL Server Business Intelligence to begin the process of building a reporting data warehouse, thereby bringing more automation and continuous improvement to the reporting process. This approach will result in improved data quality and support greater self-service reporting to enable us to continuously improve the End-User environment.

While the initial focus will be on supporting SLA Reporting, the data warehouse will provide a central repository that can support other ITSM analytic scenarios. We are committed continuous improvement

and, over time, we are will work with the County to extending both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured in terms of a number of ways, such as, increased system availability, reduced system disruptions, predictive analysis of system changes, and optimizing staffing levels.

The Four specific areas of focus are:

- Service Strategy and Improvement Analytics: This area focuses on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis
- Service Design Analytics: We see this as a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data we can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.
- Service Operations Analytics: Blending ITSM data and benchmark IT performance data, we can conduct analysis to reduce business impact of events, incidents, and problems.
- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

Additional procedures that support continual improvement include the following:

- County-159 RCA Initiation Process
- County -160 RCA SME Development Process
- County – 161RCA Team Analysis and Submission Process
- County – 162 RCA Submission Follow-up Process
- County – 175 Framework Incident Management Procedure
- County – 286 Architectural Review
- County – 314 Issue Management Process
- County – T048 Quality Management Plan
- County – T493 Business Process Re-engineering
- HPSDPP – 0121 County Change Control Process
- Problem Management Procedural Checklist (draft)

- Automated Tools – Automated systems and tools involved in proposed solution

In Table 27, we list the automated systems and tools involved in this part of the framework solution. In this environment, most tools can be used centrally for Service Desk, Asset Management, and remote diagnostics support as well as deskside by the service technician performing refresh, break/fix and IMAR tasks.

Table 27. Automated Systems and Tools

TOOL NAME AND VENDOR	DESCRIPTION
HPE Service Manager	• Part of the ITSM suite of tools • Modules provide end-to-end asset management; change, configuration and release management (CCRM); as well as an integrated solution to provide a closed loop incident process (CLIP)

TOOL NAME AND VENDOR	DESCRIPTION
Microsoft System Center Configuration Manager (SCCM)	• Overall software license management and version control • Auto-discovery of hardware and software inventory and specific user desktop configuration • Software Distribution
AirWatch	• Mobile device management • Best-in-class package according to Gartner Magic Quadrant
Microsoft Active Directory	• Used to manage the database of resources on the network
Microsoft Office Configuration Analyzer Tool (OffCAT)	• Provides a detailed report on installed Office programs • Highlights known problems
HPE Diagnostic Toolset	• Hardware diagnostics includes hard drive scanning repair, memory testing, and so forth • Supported for Win7 and Win10
Symantec Endpoint Encryption	• Full disk and removable media encryption management • Centralized management tools
Symantec Endpoint Protection 2012	• Anti-virus and anti-malware solution
HPE Asset Manager	• Provides inventory, customer, and asset information
LogMeIn Rescue	• Provides secure remote control into End-User's device, to investigate and resolve issues

We are using standardized tools in standardized configurations. This provides the best reliability in this vital set of tools.

- Qualifications and Experience – Background and experience in comparable environments

HPES is performing all of the required functions for the County today under the current contract. We have deployed best practices and meet all framework service levels, demonstrating that we have the qualifications and experience to continue to deliver these services.

HPES is an industry leader in ITSM. To remain one of the perennially top-ranked end-user service providers in the world, we must continue to lead the IT market forward. We invest $3 billion annually in research and development (R&D) to create new IT capabilities and products and develop new IT processes and services. Meg Whitman, our Chief Executive Officer (CEO), is committed to innovating and developing new IT-focused technologies: "We will continue to invest heavily to ensure that we maintain our technology advantage and align our portfolio to lead the evolution in the marketplace."

We provide several highlights from our current County service and similar engagements in Table 28.

HPES' Global Service Delivery Infrastructure

- Supports 5.4 million desktops
- Refreshes and updates more than 10,000 PCs and laptops per month on the NMCI contract alone
- Identifies more than 60 new viruses each month
- Manages more than 2 million mobile handheld subscribers
- Manages more than 4.2 million mailboxes
- Deployed more than 16 million seats of MS Exchange Server
- More than 17,000 ITIL-certified professionals

Table 28. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND ITS RELEVANCE TO THE COUNTY
County of San Diego	• We are providing these End-User Services to the County today. • End-User Services has achieved Green on all relevant Desktop Support Service Levels (56, 66, 67, 68, 69, 70, 71, 72, 73) for 2015 with the exception of missing Move Threshold – Service Level 66 for one month in February 2015; we immediately corrected that performance • We incorporate support for County Retained Assets, BYOD, and Department of Child Support Services (DCSS) customization and support more than 840 applications
NGEN	• HPES' Enterprise Service Desk (ESD) handles 97,000 contacts per month with 84% first-call resolution (FCR) rate; processes 51,000 moves, adds, and changes per month; monitors 53 Service Level Requirements (SLRs) comprising 177 separate metrics
City of Anaheim	• HPES provides on-site hardware maintenance support for 2,400 desktops, 700 laptops, tablets, printers, servers, switches, and firewalls.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

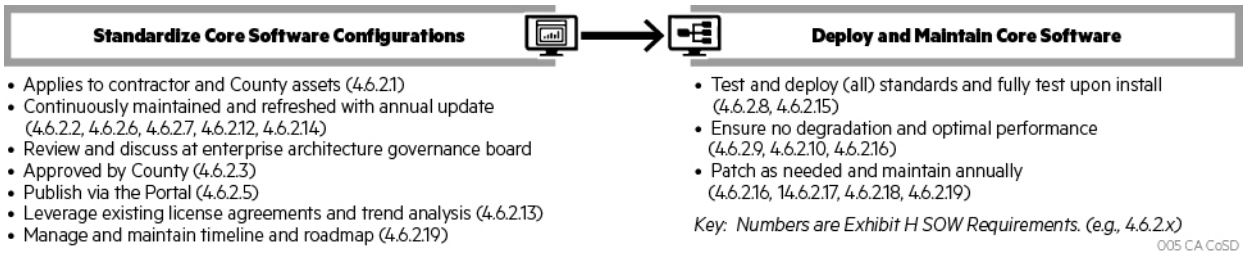
None.

Core Software Services (Sched 4.3, Section 4.6)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Core Software Services is responsible for standardizing, describing, deploying and supporting a standardized and fully tested image onto all desktop assets including county retained assets. The fundamental activities of Core Software Services can be described as Standardization Management activities and Deployment and Maintenance Support activities, as shown in Figure 51. This approach is comprehensive across all elements for the 4.6.2 High Level requirements, and these are cross-referenced to Figure 51.

Figure 51. Core Software Service Solution



Standardization is key to optimizing service

It is vital that core software configuration and updates undergo component testing, System Integration Test (SIT), regression testing, and User Acceptance testing (UAT) by the Technology Office, Applications Office, and Desktop Services organizations. Testing will be both technically focused and user "use-case" focused. Testing will also validate the security strength and integrity of the core software configuration and install. This testing is a vital step and validation that the County must verify before approving changes to the core software configuration.

Standards Enforcement and Exceptions. HPES understands the pressure from any user population to want to deviate from or supplement the standard core configuration. In working with the County, we have learned that the County would benefit with lower costs and better performance if we take a position of strength with regard to deviations from standards. Even more critical are the security vulnerabilities that non-standard software components can introduce. A standardized configuration also provides a stronger technical foundation for future transformation initiatives.

We use a process to regularly verify software versions and update as needed using SCCM, which will scan the installed base of equipment for unauthorized programs. These checks and software updates are performed automatically over the network during off-hours.

Still, users need the ability to request non-standard items. The request process and adjudication process in place will still support that. The standard test should be that a business function cannot be performed with the standard configuration—not just that the user prefers a different tool. This will help get as many users as possible onto a common platform. This standardization will ultimately save the County money. Users will have FAQs, training, videos, and other tools available to them from the Service Portal to help them learn standardized tools. The End-User Services Manager along with the Service Desk Manager will ensure all FAQ's and documentation related to the End-User environment is kept up to date on the portal and that as new applications and hardware are implemented the appropriate documentation is put in place as required. Following are three examples of approved exceptions we support today:

Department of Child Support Services (DCSS) operates on the same core software standard configuration with the addition of INFOConnect 4.1. The DCSS desktops are the predominance of County retained assets.

Public Library. In 2013, a major re-design of the Library Windows 7 image was completed and updates via login script were removed, replaced with updates being sent via the Deep Freeze console instead. This will change with the upgrade to SCCM 2016, which will allow for OS patches, software updates, and new applications to be distributed via the same tool used by the County enterprise.

Legacy Applications. To support some legacy applications, we maintain an earlier versions of the desktop core software configuration. As an example, to support Kronos, we maintain an earlier version of the desktop core software.

To help reduce the number of exceptions to the Core Software standards, we have proposed a Presentation Virtualization (Application Virtualization) Transformation project that will decouple legacy applications such as Kronos from the end-user device, allowing the overall end to progress without constraints dictated by legacy applications. Please see the Transformation Section for a further discussion of this exciting technology. Until applications such as Kronos can be virtualized, we will support the legacy applications with the approach we use today.

Rationale. Standardized core software is more efficient to deploy and maintain. It is well established via Gartner and other industry sources that the total lifecycle of any standardized configuration is cheaper to purchase, maintain, and support while still providing exceptional user service. Yet users have unique needs related to their business requirements that must be met. Our OIC approach strives to strike the right balance between standardization and optional item support. By engaging with the County in the weekly

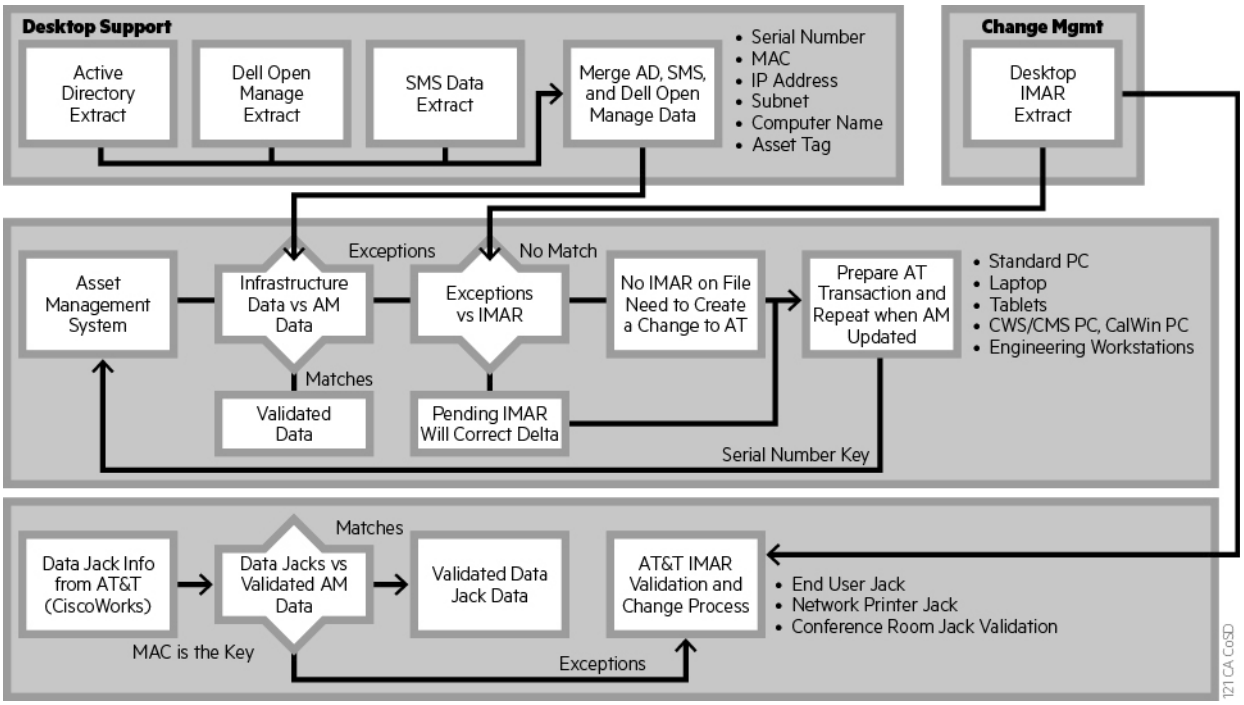
architecture meeting, the annual standards review, catalog review board, and other forums, we are confident we will continue to bring optimal value to the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The Resource and Facility approach is the same as for Desktop Computing Services. In addition to the Desktop Service Technicians, this component relies on the Project Management Office, Desktop Engineering, and Testing teams. These people are also located at HPES' Rancho Bernardo facility.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Figure 52. Core Software Services Process Flow



The desktop workflow is integrated with HPE Asset Management.

Core Software Services follow a process similar to Desktop Computing Services (Plan/Build/Operate), as described above. Some aspects with unique characteristic are described as follows.

Integration and User Acceptance Testing. This function is performed by the desktop engineering team, using onsite lab devices. This lab has access to the County and Library networks, and has many device types including the current standards and approved exceptions. When a new custom OS image or a new software package is built, testing is performed in this lab via a peer review process—meaning another member of the Desktop Engineering team performs the test to make sure it installs correctly, without errors, etc., and provides feedback/results to the desktop engineer who created the custom OS image or software package. Upon successful integration testing, if this is a Portfolio application, the HPES Application team is engaged to perform UAT. When Application team UAT is completed, the software application is provided to a small subset of County employees, who perform UAT as well. Upon successful completion of UAT, the software package is made available for production distribution to the intended user community via SCCM. If this is a catalog application, the County client who requested the application performs UAT and, upon approval, it is made available to the intended user community. If

this is a custom OS image, upon successful SIT, the image is made available to the support teams via Microsoft Development Toolkit (MDT).

Desktop Computing Refresh – Software/SCCM. System Center Configuration Manager (SCCM) is used to automate distribution of updates and to manage the overall deployed configuration. In addition, SCCM controls and prevents users from installing unauthorized software or authorized software in unauthorized configurations.

The County of San Diego has more than 15,000 HPES-managed devices (desktops and laptops), for which we provide a standard operating system, core software, catalog, and portfolio applications. Over the past 10 years, Microsoft tools have been used to create the image and to distribute software and patches to these devices. Those tools include Active Directory and SCCM for software distribution and device management along with MDT/Operating System Delivery (OSD) for OS imaging. Software refresh includes updates to the OS and applications.

OS refreshes are treated as projects and are architected for little to no interruption in the County employee's daily work. For example, during the upgrade from Windows XP to Windows 7, we deployed OSD to speed up the deployment process. This upgrade took place after normal business hours for users and was very successful.

SCCM is a solid industry-leading tool used by HPES Software Services teams across the globe. We are currently in the process of upgrading to SCCM 2016 to support newer operating systems for managed devices, improvements to the GUI, monitoring device health, and remediating client issues. SCCM automates the following core capabilities:

- Software distribution – by user, by machine; mandatory and optional (self-service)
- Asset intelligence – hardware and software inventory, compliance, application usage tracking
- Hardware and software updates – firmware and security updates
- OS deployment – for workstations only
- Scanning for equipment not detected on the network using Auto-Discovery

Using SCCM, non-emergency software updates are performed outside core hours, usually at 2:00 a.m.

For large OS upgrades within the year on a specific desktop, the software refresh methodology is more extensive and may include re-imaging the disk. Whenever possible, we try to bundle major software upgrades concurrently with hardware refresh equipment replacement as part of the annual cycle to minimize disruption to the user's work environment. Security Services for End-User Services are based on the defense-in-depth model. This model emphasizes the use of layers and multiple defense mechanisms to protect data, systems, networks, and users. In the event that one defensive measure is attacked and exploited, there are more layers and measures behind to continue to protect the assets. This results in real-time threat disruption as well as provides time to mitigate or eliminate the consequences of an event. See Section 2.5.4 Security Management Services for additional information on the defense-in-depth methodology.

- Automated Tools – Automated systems and tools involved in proposed solution

We list and describe the automated systems and tools involved in this part of the framework solution in Table 29. The table also notes HPES' value-add to the tools' utilization for the County.

Table 29. Automated Tools that Support Core Software Services Framework Component

TOOL NAME AND VENDOR	DESCRIPTION
HPE Service Manager (HPSM)	• Part of the SRA suite of tools

TOOL NAME AND VENDOR	DESCRIPTION
	• Modules provide end-to-end change, configuration, and release management (CCRM) as well as an integrated solution to provide a closed loop incident process (CLIP)
SCCM	• Automated software configuration and version management • Auto-discovery of hardware and software inventory and specific user desktop configuration • Confirmation that each county asset meets core software configuration standards for support • Security patching of OS and distribution of desktop software
Symantec Endpoint Protection / Encryption	• Antivirus, Antispyware, Proactive Threat Protection (SONAR application and device controls), network threat protection (personal firewall, host intrusion)
Forcepoint (WebSense) Data Loss Prevention	• Data loss protection on workstations (Health Information Portability and Accountability Act [HIPAA], Payment Card Industry [PCI], etc.) • Data moved to thumb drives, CDs, etc. • Data sent via Internet
Symantec Managed PKI	• Device certificates for authentication
Nessus	• Vulnerability scans of workstations
Metasploit	• Validates that security of the core software configuration is acceptable prior to addition of new components to the configuration

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

County Retained Assets Services (Sched 4.3, Section 4.7)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

County assets adhere to the same standards for configuration of hardware and software as all other assets. These machines are verified and enrolled just as all other assets. Then, County Retained Assets are serviced and supported using the same strategies, methodologies, procedures, resources, and facilities as contractor-provided assets. All appropriate service levels apply to standardized County Retained Asset Services.

Periodically, there will be a service ticket for which a user requests support on a non-standard item or non-enrolled item. In this case, the Service Desk or End-User support technician will identify this situation using the asset database. If HPES can support the non-standard item easily, we will do so as an act of immediate customer service on a case-by-case basis, with County approval.

Rationale. We have one service delivery approach for all standardized and enrolled assets that provides the best service to the user and the best value to the County. We make the same efforts for County Retained Assets as we do for contractor-owned assets.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Since County Retained Assets that adhere to the standards and are enrolled are serviced the same as contractor-owned assets, the resource and facility approach to servicing these assets is the same as it is for Desktop Computing Services and Core Software Services, as described in the preceding two sections.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

County Retained Assets are managed the same as other assets and the solutions, methodologies, and procedures described elsewhere in this framework all apply, depending on the nature of the required services. Break/fix service, however, is given only to those assets that have a Resource Unit (RU). Examples of County Retained Assets that have RUs are desktop PCs, laptops, and printers.

County assets must adhere to the standard configurations, must be "enrolled" to be on record as part of the managed configuration, and must be recorded in the asset database. When contractor support is required to "build" the software configuration for County assets, this function is performed using the same standards and procedures as described in Desktop Services and Core Software Services. Once a standardized County Retained Asset is successfully enrolled, it is managed and serviced such as any other asset. Service tickets are flagged as "County Retained Assets" so that the technician knows of the hardware status just in case there is a troubleshooting problem related to the asset's origin.

Enrollment. In order to be serviced, a County Retained Asset must be enrolled in the Service Manager (SM) asset management database. At the time of enrollment, adherence to configuration standards is confirmed. Enrollment of County Retained Assets is always verified by the Service Desk upon first service request. With the workflow to the End-User Services/Desktop Support team, the validity of a piece of equipment or configuration as being within scope has already been accomplished.

HPES currently performs these services for the County using standardized and documented procedures. We have also included reference to select procedures that protect the integrity of the configuration from non-standard, non-enrolled devices.

- Automated Tools – Automated systems and tools involved in proposed solution

Once a standardized piece of equipment is enrolled, it is supported with the automated tools that are described in all other sections of the End-User Services framework response.

We list and describe the automated tools used to support County Retained Assets a in Table 30. The table also notes HPES value-add to the tools' utilization for the County.

Table 30. Automated Tools that Support County Retained Assets Framework Component

TOOL NAME AND VENDOR	DESCRIPTION
Service Portal – myRequest – Enrollment Form	• Hosts the enrollment form, which is available to all users • myRequests will be replaced with Service Catalog and Request Manager during the Cross-Functional Transition as described in Sections 2.11 Transition Services Framework, 2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5), Special Cross-Functional Project – Replacement of myRequests

TOOL NAME AND VENDOR	DESCRIPTION
HPE Service Manager	• Modules provide end−to−end change, configuration, and release management (CCRM) as well as the integrated solution to provide a closed loop incident process (CLIP)
SCCM	• Auto-discovery of hardware and software inventory and specific user desktop configuration • Confirmation that each County asset meets configuration standards for support • Security patching of OS and distribution of desktop software
AirWatch	• Mobile device management • Best-in-class package from Gartner Magic Quadrant

- Qualifications and Experience – Background and experience in comparable environments

HPES has extensive experience providing unified and integrated support in mixed IT environments. The keys to providing support in mixed environments are discovery, standardization, and enrollment so that HPES can deliver one unified delivery model for the user.

We provide several highlights from our current County service and similar engagements in Table 31.

Table 31. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND ITS RELEVANCE TO THE COUNTY
County of San Diego	• We are providing these services to the County today. • End-User Service has achieved consistent Green on all relevant Desktop Support Minimum Acceptable Service Levels (MASLs) for 2015 while incorporating County Retained Assets • We understand how to support the exceptions to standards and County assets at DCSS, on Public Library machines, and for Kronos
City of Anaheim	• The City of Anaheim retains ownership of all its hardware and software licensing • The Anaheim IT environment serviced by HPES is a collection of more than 100 Intel-based servers running a combination of Windows Server 03 and Windows 2000, Sun Solaris, AS400, and a mainframe system. Platforms HPES supports include Visual Basic, Access, Cobol, RPG, HTML, Oracle and SQL databases as well as various commercial off-the-shelf (COTS) systems and custom software. HPES provides the following services: network, application, service desk, mainframe and mid-range computing, desktop computing, break/fix repair, system security, and disaster planning and recovery for approximately: • 2,400 desktops • 700 laptops • 1,500 mobile phones • 100 tablets • 4,000 voice stations (approximately 400 of which are on VoIP).

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND ITS RELEVANCE TO THE COUNTY
Army Computer Hardware Enterprise Software and Solutions (CHESS)	• HPES procures and supports hardware and software on this contract, which has a large number of supported configurations • HPES provides inventory management of assets and transfers of United States Army Corps of Engineers (USACE) furnished equipment—for example, software and hardware, licenses, and warranties. All computer components, peripherals, and related equipment are accountable. We developed and maintain sufficient inventory controls for accountable property, whether expendable, nonexpendable, or durable. • HPES performs routine and non-routine maintenance on desktop, laptop, and notebook software, including operating system, office automation, and COTS products, and so forth. • HPES provides hardware support for laptops, desktops, printers, servers, switches, and routers. All equipment is first analyzed, and if needed warranty tickets are created. HPES has a certified Dell technician onsite to expedite any problems on those devices and uses Cisco's warranty for switches and routers.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

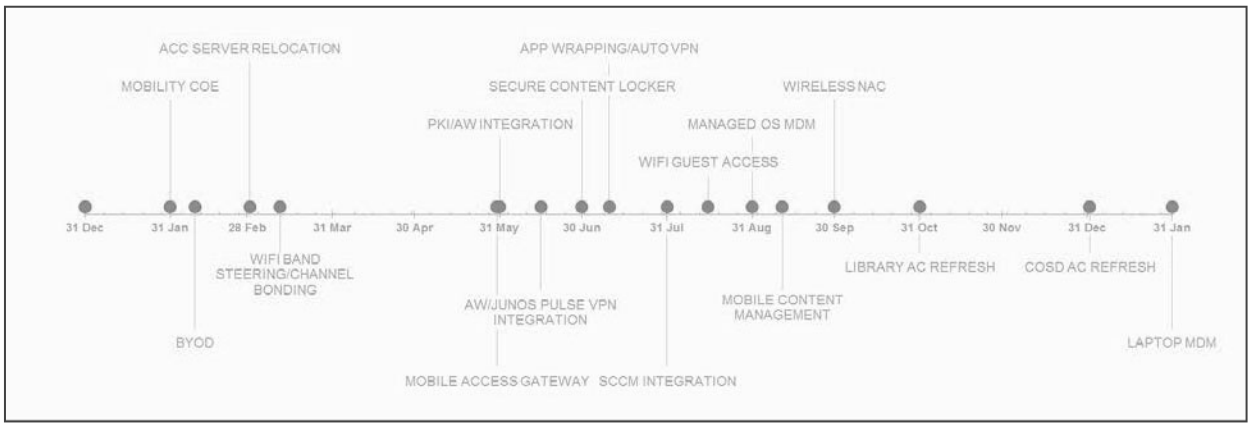
None.

Mobile Device Support Services (Sched 4.3, Section 4.8)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

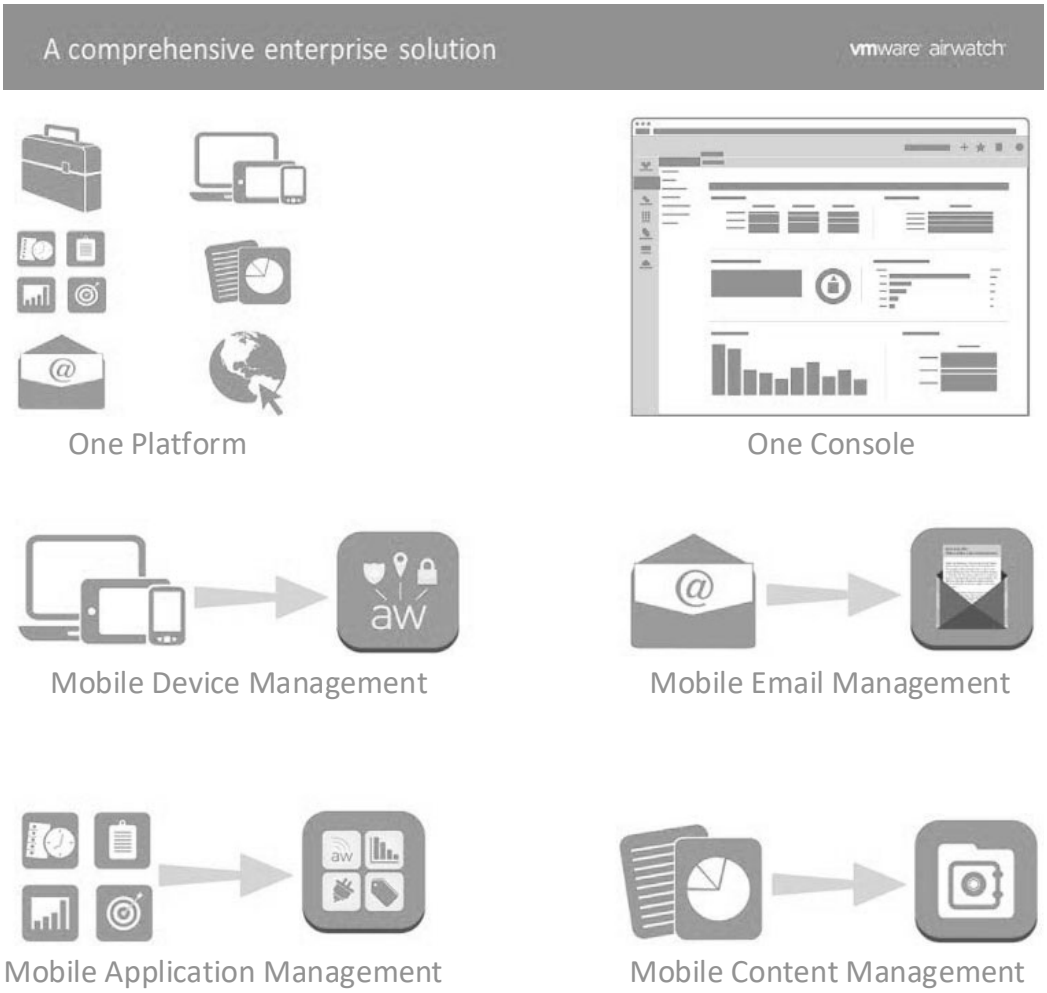
More than 3,800 County users are using the AirWatch Mobile Device Management (MDM) offering and associated support services. MDM provides policy enforcement and email access to smartphones and tablets, plus distribution of public and custom mobile applications through the County mobile application store such as Microsoft Lync Mobile and Public Safety Group's (PSG's) Probation Universal Management Application (PUMA). More recently, access to internal corporate resources—including mobile content and browser applications from MDM-managed devices—represents a new area of potential growth and business benefit to the County resulting from the County's mobilization of its workforce and the need for those users to access internal County of San Diego resources. Figure 53 illustrates the mobility roadmap jointly developed with the County, which focuses on both expanding functionality and improving operational processes surrounding the mobile environment. This roadmap is currently under revision for 2016 and beyond.

Figure 53. 2015 Mobility Roadmap Milestones Jointly Developed with the County



The support model for MDM is focused on enabling the mobile user using the specific capabilities offered by the AirWatch platform—shown in Figure 54. All initial enrollment and other support requests are made to the HPES Service Desk—always the first touch and owns the service ticket for the entire life of the ticket open through close. The Service Desk validates the user's information and offers information and support that may solve the problem. For all mobile services that require AT&T support, the user's ticket will get a "warm handoff" to the AT&T helpdesk. AT&T's helpdesk will provide a single AT&T point of contract through each service transaction, even when AT&T needs to access multiple support organizations. AT&T support handles certain issues either by the local AT&T Incident/IMAR managers or by the AT&T Mobility Solution Services (MSS) and AirWatch partners. These user requests include Device Enrollment or Registration, Passcode Reset/Unlock, Lock Device, Locate/Find, Add/Delete Users, Device Enrollment (bulk or individual), and Device Wipe. The one component missing from this support suite has been the mobile device and its operating system as well as any mobile carrier issues the user may encounter. Today's County mobile user still must place a second call for problems that are not MDM related. Examples include cellular carrier issues and those of device manufacturer (e.g., iPhone or Samsung) or device operating system issues.

Figure 54. Capabilities Managed by the Airwatch MDM Solution



AirWatch is the single key tool to manage all MDM activities.

To expand support, we are proposing a fully managed Mobile Device Support Service that will provide comprehensive operational support of all County-provided mobile devices as well as County resources that are available on BYOD devices. As an additional support offering from your Service Desk, this new service will provide County users with single point of contact for AT&T's MDM support, using a multi-tiered model designed to handle any type of mobility support need—mobile application, operating system, content management, device familiarity, email access, and even carrier related issues. The AT&T Enterprise Mobile Support team will resolve AirWatch MDM, device/OS, and carrier-agnostic mobility issues in response to County user-generated trouble tickets logged with the HPES Service Desk. This team provides expertise and support for most current mobile devices and accessories and will directly engage the end user in the diagnosis and resolution of their issues or will route requests to the appropriate support organization if required. They will also provide a "warm transfer" for County users for those issues requiring wireless carrier intervention. Throughout the process, this team also provides ticket management and communications through the HPES Service Portal so that service levels are accurately tracked and the user is kept informed of the status of the request throughout its lifecycle. If the ticket requires further technical intervention, it will be escalated through additional tiers of MDM support by AT&T.

The support structure for mobility has the depth and breadth to deal with any user issue. From a user perspective, their mobility issues will be managed by a team with a robust network of support "behind the curtain" that is made up of subject matter experts so that problems are driven to resolution.

Here is a summary view of each group's responsibilities:

AT&T Enterprise Mobile Support Team

This group is the AT&T front door for all mobility provisioning and/or break/fix activities. They will interact directly with the end user on all MDM-related issues and provide the basic support and continuity of support for issues such as Device Enrollment, Device Lock and Wipe, etc. Additionally, as mentioned, this team will provide general device and operating system support as well as facilitate warm transfer to the carrier as the need is identified. For the large percentage of issues, they will provide first-call resolution. For the remainder of these tickets, they will also act as the coordinator for the report if it requires escalation to one of the technical support organizations.

AT&T LCM Trade Street Service Desk

This group is our existing MDM support staff. This group will continue to maintain overall responsibility for ticket management and service level attainment for MDM actions. As part of the ticket flow, they will also provide the interface to HPES for custom mobile application support, Active Directory, and Outlook email Exchange group issues.

AT&T Mobility Solutions Services (MSS) Application Service Desk

This Application Service Desk provides leveraged technical support to AT&T Enterprise Mobile Support team via phone, email, or internal AT&T portal for additional MDM support services. Responsibilities include advanced troubleshooting, isolation and resolution, application use, and configuration support as well as MDM managed services requests.

AT&T ASD/MSS Service Assurance Team

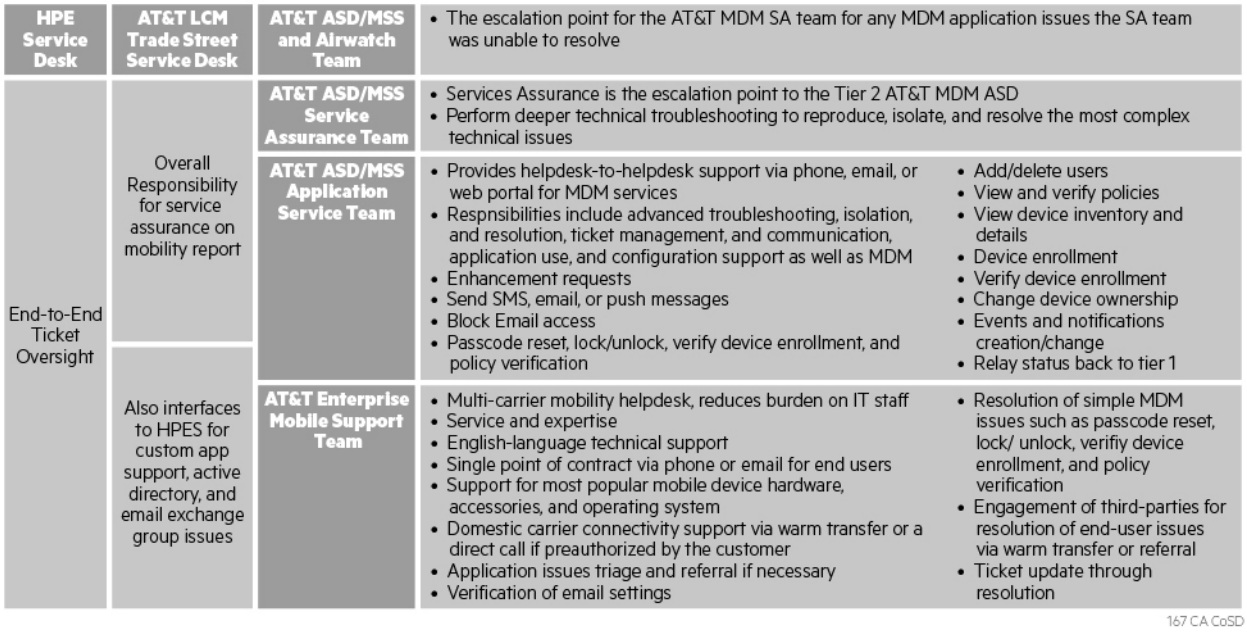
This is the first-level technical escalation point to the AT&T MSS Application Helpdesk, which performs deeper troubleshooting to reproduce, isolate, and resolve the most complex technical issues.

AT&T ASD/MSS and AirWatch Mobility Consultant Teams

The escalation point for the AT&T ASD/MSS Service Assurance Team, which involves the AirWatch vendor technical team for any MDM application issues requiring the highest level of analysis and support.

Figure 55 provides more detail on the organizational roles for the mobile solution.

Figure 55. MDM Support Model



We have an integrated and comprehensive MDM support service model

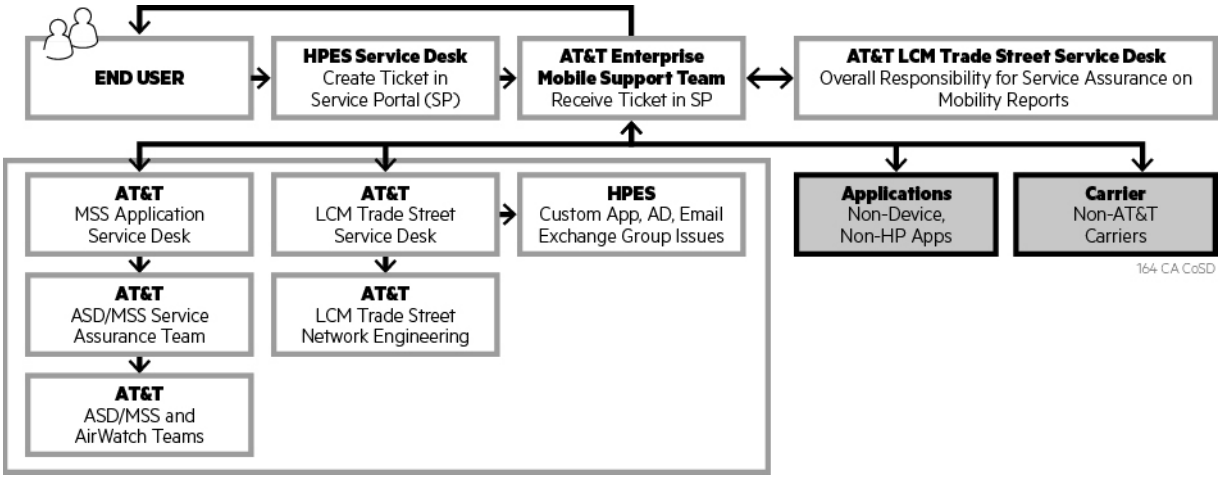
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

AT&T will leverage the local Life Cycle Management (LCM) team, the AT&T Enterprise Mobility Support team, and the AT&T Application Service Desk (ASD) organization. AT&T LCM personnel are located at the AT&T facility in San Diego. All other personnel and facilities are located at leveraged sites around the U.S.; this leveraged support will be transparent to the user. The County's MDM infrastructure is hosted in the AirWatch shared cloud and interfaces with County resources through a geo-redundant AirWatch Cloud Connector configuration located at both the AT&T Point of Presence (POP) and the County Operations Center (COC). Smartphone users who are using BYOD can, of course, get additional service related to their devices overall at their service provider's walk-in retail location, including AT&T locations for AT&T subscribers.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The major difference between today's support model and the one to be implemented once the Managed Mobile Device Service is in place is that the same set of tools and processes currently used by the LCM Incident/IMAR desk will be replicated for the Enterprise Mobile Support team. They will have access to the HPES Service Desk ticketing platform used for break/fix reports and will be able to status and resolve tickets generated by the HPES Service Desk. They will also follow existing procedures in using the AirWatch console for MDM related problems. The HPES Service Desk Tier 1 agent maintains end-to-end ticket tracking, maintaining automated and chat communication with the AT&T service desk for MDM, mobile device, and wireless carrier issues. The LCM team will continue to meet service level responsibilities and will follow all reports to closure. Figure 56 illustrates the organization of Service Desk components for mobile users.

Figure 56. County of San Diego Mobile Support Services Methodology



Internally, our support has clean lines of accountability and service that are transparent to the user.

AT&T currently performs these services for the County via standardized and documented procedures as shown in Table 32.

Table 32. Standard Documented Procedures

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
AirWatch – MDM AT&T Incident	Once ticket is received, or warm transfer of caller from HPES Service Desk after AD password and role has been verified, Tier 1.5 will work with the end user to fix the issue. If Tier 1.5 cannot resolve the issue, it will be given to Tier 2 to be worked through to conclusion. The incident manager will document in HPE Service Manager, and transfer the ticket to the correct group to fix the issue or resolve the ticket.	AirWatch Console
AirWatch – MDM AT&T IMAR	Once an IMAR is created, IMAR Manager will review line item and ensure user appears in the AirWatch Portal correctly. Monitor to ensure other line items are closed by HPES and send out instructions to the requester for AirWatch app install and configuration. Working with end user on deleting the old device when requested. IMAR manager documents change in the IMAR and close.	Airwatch Console

- Qualifications and Experience – Background and experience in comparable environments

All AT&T and partner organizations and personnel for the Mobile Services solution are involved in MDM and Mobility implementations worldwide. The LCM team has supported the County since the rollout of the current Agreement in 2006 and has been provided MDM services since they were migrated to the Airwatch platform in 2014.

AT&T's MDM solution is provided to thousands of corporate and government customers globally. AT&T's AirWatch MDM shared and dedicated hosted solution currently supports connectivity to over 100,000 devices.

In Table 33, we provide several highlights from our current County service and similar engagements.

Table 33. Qualifications and Experience that Substantiates our Ability to Perform for MDM Framework Component

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND ITS RELEVANCE TO THE COUNTY
County of San Diego	• We are providing comprehensive MDM support to the County today using AirWatch • We incorporate County Retained Assets, BYOD, DCCS customization and support hundreds of applications
Orange County Sheriff's Department	• AT&T currently offers and supports AirWatch Mobile Device Management services much the same as the County of San Diego for the Orange County Sheriff Department. The Orange County Sheriff Department currently has 1500 corporate owned devices and 1100 BYOD devices enrolled and managed by the AirWatch hosted solution with access to corporate resources such as email, contacts and calendar.
Department of Housing and Urban Development (HUD)	• HPES uses AirWatch to support MDM - We manage HUD's wireless and mobile device environment for more than 1,600 end users. Mobile End User Services we provide include setup, maintenance, monitoring, application provisioning, and access provisioning. Mobile platforms we support include Blackberry, iOS, Android, and Microsoft Surface devices. We have used several different mobile device management (MDM) tools including: BlackBerry Enterprise Server, Good for Enterprise, Good Mobile System Management/Boxtone, and AirWatch.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Unified Communications Services (Sched 4.3, Section 4.9)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES and, AT&T, in conjunction with industry-leading software/application vendors and the County, are presently planning, deploying, and activating Unified Communications (UC) Services, which enable improved collaboration capabilities across each business area in the County. These UC capabilities include O365, Lync/SfB, Mutare Enhanced Voicemail for voicemail to email delivery as well as Avaya's EC500, which extends both internal and external calls to a County user's desk and/or a mobile phone provided by the County. UC capabilities will be delivered users on their computer, tablet, smartphone, or VoIP handset. In reality, this integrated functionality requires the use of fully integrated application services hosted within the PoPs, data centers, and the cloud. These technology enhancements are continually blending and enhancing previous standalone solutions. For instance, using Avaya EC500 Extension to Cellular, calls now ring on the user's desktop/handset as well as their smartphone, enabling a conversation despite the recipient being out of office or the caller had to hang up and call the recipients

mobile number. Mutare's Speech to Text (STT) capability also allows the user to access email and connect to voicemail by receiving a text interpretation of the message with an embedded audio file. These solutions have allowed early adopters to take advantage of UC capabilities, enhancing the user experience and improving County productivity. For example, voicemail can now be delivered in email, eliminating the need to separately dial in to voicemail.

HPES has been delivering UC capabilities to the County since 2013 and our solution proposes continued transformation of these services while leveraging the deployed solutions. Table 34 highlights UC services already active or in-flight within the County and identifies UC capabilities to be transformed.

Table 34. US Services Already Active or In-flight

CURRENT CONTRACT CAPABILITIES	PROPOSED NEW CAPABILITIES (BY THE END OF TRANSITION)	TRANSFORMATIONAL (AFTER COUNTY APPROVAL)
• Mutare Voicemail to Email with SST • Avaya IP softphone • Avaya Extension to Cellular • Avaya IP soft phone for agents • Avaya Enterprise Directory Integration	• Avaya Communicator for Lync • Avaya Collaboration Services for Outlook/ Browser/ Microsoft Office	• Avaya Communicator SIP mobile client • Avaya Presence Services

Office 365 Components

Through the County-licensed Microsoft Office 365 cloud offering, which includes Lync/ (Skype for Business), users will have access to instant messaging, presence, web conferencing, video conferencing, desktop sharing, and interactive whiteboards.

Table 35. Specifies when the County will receive the various components of O365

MODULE OF O365	CURRENT CONTRACT CAPABILITIES	NEW (BY END OF TRANSITION)	TRANSFORMATIONAL (AFTER COUNTY APPROVAL)
Lync and/or SfB	Y (Lync)	Partial SfB	Full SfB by 2018
OneDrive	Partial	Partial	Integrated
O365 Office Apps	Y	Continued Y	Continued Y
eMail	N	Y	Continued Y
SharePoint Online	N	N	T&M

Avaya Integration with Lync (Skype for Business)

With the planned deployment of Avaya Communicator for Lync during 2016, users will be able to move from limited peer-to-peer audio capabilities into conferencing capabilities hosted within the Avaya Enterprise voice network. As UC services progress, desktop web conferencing capabilities will become fully interoperable with conventional Cisco teleconferencing platforms.

Other UC capabilities to be implemented include using Avaya Communicator for Lync and collaboration services, which contain plug-ins for Outlook, and providing complete call control from the Lync or SfB client with the following key features:

- Click to Call On-Net and Off-Net local and long distance calls, using your computing device, mobile, or desktop telephone set
- Click to Answer incoming calls from Lync or SfB, using your computing device, mobile, or desktop telephone set
- Search and Click to Call internal and external County contacts from Outlook email
- Screen pop with contact on incoming calls from Outlook contacts.

Speech to Text (STT) Integration

Another related feature of our solution is the continued use of the existing Mutare Enhanced Visual Messaging with STT service. This solution transcribes a user's new voice mail message into text via email along with a .wav attachment or a secure web link for streaming the message to the County end-user email via SMTP relay.

Mobile Unified Communications

We will continue to leverage the AirWatch SaaS MDM solution for deployment of UC mobile (e.g. Avaya mobile client, Skype for Business) applications to the County of San Diego mobile application store for corporate owned managed devices, as well as, upon approval, employee owned BYOD devices. Once the UC mobile application has been deployed, whether on a corporate managed device or an employee owned BYOD device, HPES and AT&T will provide full support of the application and its connectivity and functionality to the systems that provide these UC capabilities as references in sections 4.8 for Mobile Device Support Services and 5.11 Mobility Infrastructure Services.

Through the integration of the AirWatch Mobile Device Management (MDM) and the Symantec Managed PKI solution for deployment of PKI payload profiles, all corporate managed and BYOD mobile devices and users can now be authenticated prior to accessing UC services or resources. This will allow for County mobile users to take advantage of the Lync/SfB mobile application, which provides presence, instant messaging, and other capabilities while on the go. Additionally, through Avaya's Communicator for Mobile application, users will be provided with full enterprise telephony functionality from their mobile device, allowing them to make, receive, transfer, and put calls on hold as well as use advanced features such as Active Directory (AD) lookups and presence status from Avaya voice and SfB users. Users will have Full Call Control in addition to common enterprise voice features, such as:

- Make/receive calls
- Hold/retrieve calls
- Transfer calls
- Multiparty conference calls.

UC Data Sharing

UC data sharing will also evolve from traditional SharePoint and network file share capabilities to enterprise file sharing and synchronization.

- **Email** – This is currently provided by HPES for all County employees but will be migrated to Office 365 Exchange Online during the transition phase of the new Contract.
- **SMS** – This feature is part of the mobile device services and may be provided by the carrier of choice by business unit. AT&T, for example, has an outbound SMS application service in place for the CalFresh group of HHSA. This is a hosted service and is isolated to the business unit and is not available to the enterprise.
- **Fax** – Local and premise-based fax services are either provided by the Avaya PBX or separate 1 MB lines by AT&T Core—are all supported by AT&T life cycle management (LCM). Additional fax

capabilities are offered by HPES via the Right Fax solution, which will be integrated with Office 365 Exchange Online. This solution provides users with fax to email services.

UC Support

HPES understands the critical need for UC support services that operate in conjunction with each new service deployment. While the user community may be eager to use a new UC feature, they will not be instantly proficient. As such, our proposed solution includes front line support as a part of both our Service Desk Services and End-user Services. Support and training resources are also provided through the Service Portal. We will continue to leverage our previous Service Desk activities as well as develop, update, and maintain Service Desk scripts and processes for the UC user community. During this next contract, and in direct support of these new unified capabilities, HPES proposes posting training videos. These are frequently preferred over text-based training and are part of our efforts to continually develop and update training documentation and end-user tip sheets for Service Portal posting. As with all our Service Desk activities, our UC support includes incident tracking, escalation, and resolution.

Teleworker and Remote User UC

We will deploy, after County approval, Avaya Communicator integrated UC and voice services clients. These integrated clients will provide the current 2,600+ users, and any future SSL VPN County users, access to a complete, consistent, and rich set of capabilities both on-net and off-net. Avaya Communicator desktop and mobile clients can operate in both VPN and non-VPN mode to provide remote connectivity. Avaya's Session Border Controller, in conjunction with Client Enablement Services, will allow users of Avaya communicator clients (desktop or mobile) to operate in SIP (session initiation protocol) mode. Enterprise security standards, such as TLS and SRTP (secure real-time transport protocol) encryption, will provide effortless access to UC and voice services integration, enabling teleworkers to function as if they are in the office regardless of their location.

Software and Release Management

Our subject matter experts (SMEs) will subscribe to Avaya's UC integrated client updates, service packages, or version upgrades. These will be thoroughly reviewed by SMEs for County environment relevancy and tested in a lab environment before production deployment is recommended. This standardized process will validate production functionality of any recommended new release update, service package, or version upgrade so that the County user environment is not disrupted or compromised.

AT&T SMEs will apply industry standard software release management methodologies to support standard version delivery and consistency across all County users' devices and assets. These standards will apply to Avaya One X Communicator, Avaya Communicator for Lync/SfB, Avaya Communicator Mobile, Avaya One X Agent, and Avaya Collaboration Services. The same applies to any proposed applications that will need to be deployed to the County's managed mobile devices via the AirWatch MDM solution.

We will create, post, and document consistent UC client software packages for all client types.

This process will integrate with all ITSM processes in place to ensure communication, approval, etc. and full integration with the overall program.

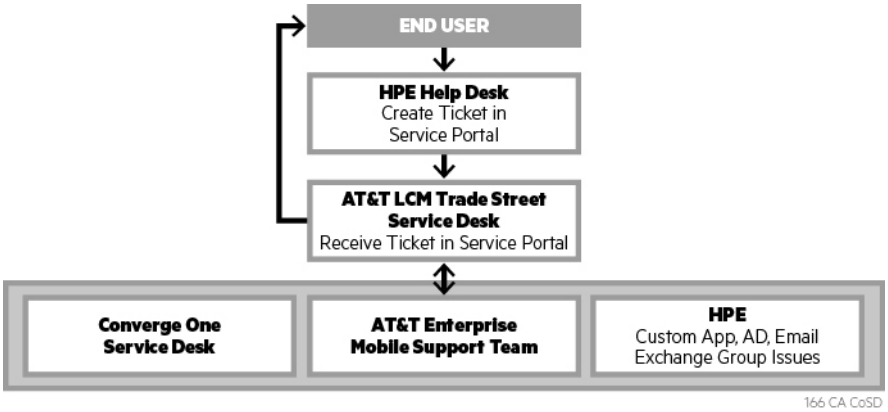
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

As with other services, the County will use HPES Service Desk to support UC. We have high-tier support with both AT&T and Microsoft. Note, however, that our Service Desk will still own support tickets through the entire life cycle for the convenience of the County.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

All support services, whether triage, new requests, change requests, or removals will be initiated by the County user to the HPES Service Desk. All requests that are within the network framework for real/non-real time services will be directed to the AT&T LCM team for assessment and completion. Figure 57 illustrates our support services methodology.

Figure 57. County of San Diego Unified Communications Support Services Methodology



AT&T's Service Desk is fully integrated with HPES so the user always initiates their ticket with the HPES Service Desk.

Table 36 delineates services HPES currently performs for End-Users in accordance with the standardized and documented procedures.

Table 36. Services Currently Performed by HPES for End-Users

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
Mutare EVM Incident Request	Documented process for user request to repair trouble with Mutare EVM service	Service Center
Mutare EVM IMAR Request	Documented process for user request for active or new service for Mutare EVM	Service Center
Avaya IP Softphone Incident Request	Documented process for user request to repair trouble with Avaya IP Softphone service	Service Manager
Avaya IP Softphone IMAR Request	Documented process for user request for active or new service for Avaya IP Softphone	Service Manager
Avaya Extension to Cellular Incident Request	Documented process for user request to repair trouble with Avaya Extension to Cellular service	Service Manager

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
Avaya Extension to Cellular IMAR Request	Documented process for user request for active or new service for Avaya Extension to Cellular	Service Manager
Avaya IP Softphone for Agent Incident Request	Documented process for user request to repair trouble with Avaya IP Softphone for agent service	Service Manager
Avaya IP Softphone for Agent IMAR Request	Documented process for user request for active or new service for Avaya IP Softphone for agent service	Service Manager

- Automated Tools – Automated systems and tools involved in proposed solution

For quality UC support, our SMEs will use numerous automated tools. These tools enable us to continuously monitor the overall health and performance of voice appliances, assist in rapid restoration through fault isolation, and perform traffic analysis as shown in Table 37 and discussed further below.

Table 37. Tools Which Enable Continuous Monitoring of the Overall Health and Performance of Voice Appliances

TOOL NAME AND VENDOR	DESCRIPTION
Avaya Expert Systems	Avaya maintenance services include Avaya Expert Systems and Secure Access Link (SAL). Avaya Expert Systems provides the County with Core Voice Services, a maintenance database of more than 30,000 artificial intelligence algorithms (AIAs) with scripted automation. These scripts automatically correct many known system- and software-related issues.
Avaya Secure Access Link (SAL)	Avaya SAL is a centralized consolidation point for all Avaya core systems for health and alarm monitoring, secure remote access using secure outbound- only HTTPS , and an integration point for Avaya Expert Systems.
Nectar's Unified Communication Management Platform (UCMP)	UCMP and its complete suite of innovative features will provide the County enhanced, integrated UC network services. Nectar provides multivendor management services including application dependency, tree visual alerting, and vendor knowledge modules, which help our SMEs proactively pinpoint and resolve cross-platform integration issues quickly and restore services to County users.

HPES will deliver complete manufacturer system maintenance coverage on all County Core Voice Services assets. Together, these tools provide complete health monitoring and expeditious issue resolution. Avaya Expert Systems and Secure Access Link are online and engaged 24x7 to diagnose and attempt to resolve known system alarms, clear many service affecting issues, and escalate to engineering resources for prompt attention when necessary.

Our UC team will use Nectar's UCMP and its complete suite of innovative features to provide the County enhanced, integrated network services. Nectar provides multivendor management services including application dependency tree visual alerting and vendor knowledge modules, which help our SMEs proactively pinpoint and resolve cross-platform integration issues quickly and restore services to County users. The UCMP also includes real-time network quality of service reporting using RTCP integration, and can create simulated traffic injection between designated network segments for analysis. This allows the SMEs to monitor and report on all VoIP related traffic transmissions.

The quality of service reporting tool provides per-hop statistics and in many cases assists in quickly identifying improper packet handling hop points. This drives the efficient resolution of network quality of service issues. The Nectar platform includes statistical resource utilization data gathering and storage that enables trending analysis and capacity planning so that County users are not impacted by growing resource needs. Finally, these capabilities will be available using an intuitive and customizable dashboard with visual and electronic alerting from sophisticated threshold configurations. The dashboard allows us to acknowledge, respond, and correct issues proactively, in many cases before County users know or report an issue.

- Qualifications and Experience – Background and experience in comparable environments

In Table 38, we provide several highlights from our current County service and similar engagements.

Table 38. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND ITS RELEVANCE TO THE COUNTY
County of San Diego	• We are providing these exact services to the County today. • End-user Service has achieved 100% or Green on all the relevant MASLs for each of the last 12 months. • We incorporate County Retained Assets, BYOD, DCCS customization and support over 840 applications
Orange County Sheriff Department	• AT&T currently offers and supports AirWatch Mobile Device Management services much the same as the County of San Diego for the Orange County Sheriff Department. The Orange County Sheriff Department currently has 1,500 corporate-owned devices and 1,100 BYOD devices enrolled and managed by the AirWatch hosted solution with access to corporate resources such as email, contacts and calendar.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Catalog Services (Sched 4.3, Section 4.10)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Solution Summary. The Optional Item Catalog (OIC, currently referred to as the Optional Item Purchasing Catalog [OIPC]) holds all approved single user applications, standard and nonstandard hardware items, and support only services.

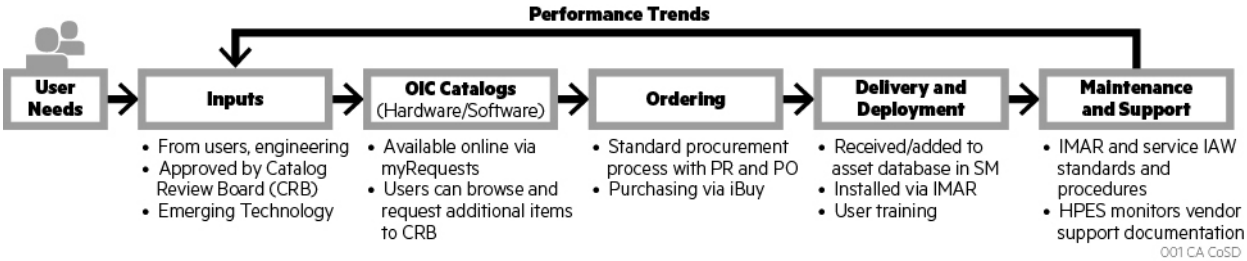
To implement this solution, the configuration of the catalog will be controlled by the Catalog Review Board (CRB). The board consists of HPES and County selected points of contact (POCs) from each department to discuss, review, and approve items for inclusion in or removal from the catalog.

Catalog activities, such as ordering, maintenance, and approval, will be accessible online via the Service Portal and myRequests. While all users can order, only select users can perform other functions—review and approve, for instance—based on their organizational role and authority. myRequests will be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in Section 2.11 Transition Services Framework, 2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5), Special Cross Functional Project – Replacement of myRequests.

Requirements and requests for new catalog items or updates can come from users, engineering analysis, and new technology offerings from HPE, third-party vendors, and elsewhere. County desktop hardware peripherals, laptop accessories, stand-alone printers, and desktop software prices are reviewed on a quarterly basis by HPE Global Procurement through a Request for Quote (RFQ). We check with suppliers to compare prices and delivery schedules to match the existing catalog and make the necessary changes, often resulting in lower pricing. Once the catalog manager receives the updated list from HPE Global Procurement, he/she updates the OIC. The updated list is reflected in the following OIC publication, which occurs on the 20th of every month. The catalog is updated with new end-user hardware peripherals and end-user software, including pricing on these items, one for hardware replacement and one for end of life (EOL) hardware.

Figure 58 provides a summary of the OIC solution—rom identification of item need to delivery and support.

Figure 58. The OIC Process



Continually refreshing, maintaining, and supporting the existing catalogs is vital to the effectiveness of this framework component.

Once approved, the catalogs are available via the Service Portal. Users order via myRequests using functionality described in the "MyRequests User Guide."

For nonstandard items that are already installed and deployed, we will support OIC items through the warranty period for hardware. Only standardized items that have an approved Resource Unit (RU) will be supported outside of the warranty period through the standard process. If additional assistance is needed, we have other processes in use today— Nondiscretionary work request (NDWR), Very low risk (VLR)—that provide the support for these items. These options will remain in place going forward to make sure support requests escalated to HPES can be addressed and put the end user back in service as quickly as possible.

User training will be available on OIC items, as necessary. OIC items are monitored by HPES for manufacturer updates and are incrementally refreshed as recommended and approved. Specialized user support for applications will depend on the nature of the applications and the problem. Technical and configuration support will come from HPES' break/fix technicians. If the issue is determined to be related to an application with a Portfolio Application Identifier (PAID), identifying it as a supported application, HPES' Service Delivery Manager (SDM) for the business unit will work with the vendor and the County apps owner for that portfolio application. Refresh is not included with OIC items that do not have a support RU; a new order will be required.

Each item in the hardware and software OIC catalogs will be sorted by category, with a brief description, manufacturer, model/reference, and a unit price. For commercial items, pricing is set competitively via our procurement organization in agreement with the RFP requirements. If a user selects an item that requires End-user Service support for installation, those requests are added at the end of the optional item ordering process.

On the software side, there are currently three categories of desktop software:

- Purchase - Software products that are available for purchase and are delivered to you by HPES.
- Supported but no longer available for purchase – Software products that are part of the Desktop Application Directory but are no longer available for purchase (for example, old versions of software). These products are still supported by HPES.
- Other desktop software - Software that can be installed if licensing is in place. An analyst contacts you to discuss licensing before the software is installed.

Overall, the OIC catalog has more than 1,700 line items. OIC is focused on applications (approximately 440) and portfolio applications (approximately 350). Standard Core software items are listed in Report 43.

Rationale. Catalogs such as the OIC provide a mechanism for users to buy validated and necessary items and services are that not part of the core configurations for desktop peripheral hardware, stand-alone hardware, desktop software, portfolio application client software, and IT training courses. This provides users with stability and cost savings of a standardized core system configuration as well as an opportunity to purchase supplemental (that is, optional) items when needed.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The OIC will be available via the Service Portal in myRequests, both of which reside on servers at the HPES data center. OIC management and deployment/service of optional items involves HPES resources in management, engineering, procurement, and end-user services, most of whom are assigned to the Rancho Bernardo data center. Others are part of a virtual team from across the U.S.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

As a note, OIC and OIPC are synonymous terms in usage

Online Catalog. The OIC lists items available for purchase by County users and contains standard items from Report 43 and 44, as well as optional items. Users can shop for items available for one-time purchase or RUs (monthly fee), including bundled services. Users can also suggest changes to the catalog. When an item is approved and an order is placed, HPES fills the order and delivers the products to the requester. HPES will:

- Coordinate an installation appointment with requestor
- Assist with set-up, including physical installation and connection of the device to the workstation or network
- Assist with the initial loading of the software products listed in the catalog,

The OIC is accessed from the myRequests page, which resides as a link from the Service Portal.

Viewing/Modifying Catalog Requests

All catalog requests will be viewable by the requestor but can only be modified prior to submission. If a change is needed after submission, the user will need to clone the request, and then make the changes.

After the changes are made, and old requested is no longer need, it can be deleted. To see the purchased status of an item, the user can click the Purchasing tab.

Reviewing and Authorizing Catalog requests. If a user is a reviewer for the Catalog, they can access requests that have been submitted. These requests appear on the Review Catalog Requests screen. After accessing a request, the reviewer will make comments that are then sent back to the requestor, rejecting or approving the request as submitted.

Shopping from the Catalog

A user can order hardware, software, or services from the catalog including video conferencing equipment, audio-video equipment, and telephones, computer and phone services, or special bundles for new employees. For all catalog orders that involve site installations, they must be authorized by the County Technology Office, who will be notified by the myRequests system.

Billing, Authorizer, and POETA

After a request is made, the user will be prompted to enter their billing and authorization information. myRequests will use this information to "file" the request with the appropriate County agency and provide the correct financial account management. Each letter in the word "POETA" stands for a different billing item. The user should contact the financial coordinator of the business group for the correct information to submit. Billing will be in accordance with the supplied POETA information.

Procedures. HPES currently performs these services for the County today via standardized and documented procedures.

The process to manage the catalog is straightforward and has been very successful. Catalog updates are managed in coordination with other standards governance activities, including the annual standard desktop configuration update and the weekly architecture review meeting. The catalog is updated in synch with other configuration changes.

The key to continual improvement in the Catalog Services component is to perform benchmarking with vendors, making sure that the catalog is refreshed regularly, is responsive to user needs, and that catalog optional items integrate and interoperate well with the standardized core configurations. Each new component is SIT and UAT tested and approved by the County.

- Automated Tools – Automated systems and tools involved in proposed solution

The automated systems and tools involved in this component of the framework solution are described in Table 39.

Table 39. HPES' Value-Add to the Tool's Utilization for the County

TOOL NAME AND VENDOR	DESCRIPTION
Service Portal including myRequests	• Web-hosted online "one-stop shop" for service and product requests • myRequests will be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in Section 2.11 Transition Services Framework, 2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5), Special Cross Functional Project – Replacement of myRequests

TOOL NAME AND VENDOR	DESCRIPTION
Service Manager	• Modules provide end-to-end asset management, change, configuration, and release management (CCRM), as well as an integrated solution for providing a closed loop incident process (CLIP).
SCCM	• Automation of core software license and configuration management • Auto discovery of HW and SW inventory and specific user desktop configuration • Confirmation that each County asset meets configuration standards

- Qualifications and Experience – Background and experience in comparable environments

In Table 40, we provide several highlights from our current County service and similar engagements.

Table 40. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND HOW ITS RELEVANCE TO THE COUNTY
County of San Diego	• HPES manages the OIC (OIPC) for the County today, providing procurement, support, and testing for all items. • HPES has met all service levels related to the Catalog; new catalog requests are accepted and approved throughout the year
NGEN	• HPES provides a web based product services catalog integrated with ecommerce functionality. We maintain automated interfaces between the Government and our ordering systems. • Approvals are managed in the Government system with delivery initiated in our systems. • We populate our service catalog as we add request management workflows over time with the automated workflows triggered by catalog requests. This processes also provides for continual improvement of catalog content.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Network Printer Services (Sched 4.3, Section 4.11)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Network printers are an integral part of the existing standard configuration and will be integrated into the user service model and network architecture seamlessly. Managing network printers is a core systems administration and maintenance task for all of our technicians. We currently support a diverse set of network printers as shown in Table 41.

Table 41. HPES' Current Support of Network Printers

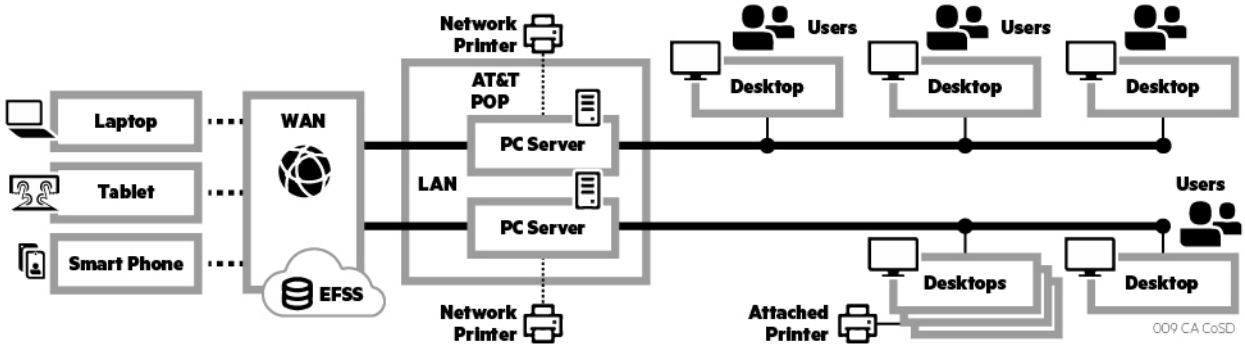
PRINTER TYPE	QUANTITY SUPPORTED (AS OF MARCH 2016)
Monochrome Network Workgroup Printer – Standard Format	735
Monochrome Network Workgroup Printer – Large Format	52
Monochrome Network High Volume Printer – Large Format	19
Color Network Workgroup Printer – Large Format	45
Color Network Workgroup Printer – Standard Format	191

The network printer support solution is the same for all types of printers. The only difference is in configuration and utilization information related to specific makes and models of printers. Figure 59 below summarizes the network printer configuration.

Network printers are standardized attached devices and are operated and maintained under many of the same procedures for hardware and core software. Desktop services handles the printers, their configurations, drivers, and the queues. The local server team manages the print servers located in the AT&T POP and in the DR POP location in San Diego, as well as other locations where servers are installed throughout the County (such as FRCs and CAC).

HPES is currently providing network printer services support and meets all related service levels.

Figure 59. Network Printer Architecture



For reliability and performance, we use a standard network printer architecture.

Rationale.

We are taking steps to realize savings and efficiencies for the County as described in the experience subsection. For example, we recently completed a printer/server rationalization and upgrade, improving redundancy and resiliency for end users. We will continuously look for ways to improve print services and their value to the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

We will perform this work from our Rancho Bernardo facility.

All service technicians have basic training and skills in network printer operations, maintenance, and troubleshooting. We have a hardware team that specializes in printer/server support but all field

technicians are trained at a basic level to support these devices. Printer specialists are embedded in the Desktop Services organization but are not a separate team.

Our technicians have the same core skills but different levels of expertise in specialized areas, such as surge and DR situations. Because of this, we are able to cross-assign staff to a critical area. This human resource strategy provides constant, consistent, and surge service to all County IT users.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Printers are a specialized device on the network, but the overall processes and procedures described previously in the end-user framework apply to printers. Printer management involves printer specific activities such as:

- Printer service IMAR and operations
- Printer device management
- Queue setup
- Load balancing
- Printer security management
- Configuration setup and management for groups and individual users.

The requirements to support network printers are part of our plan, build, operate approach. Table 42 maps each of the framework component requirements into a Plan, Build, Operate (PBO) phase and then summarizes HPES' solution and methodology and key processes.

Table 42. Mapping of Framework Component Requirements for PBO Phase

STAGE	COMPONENT REQUIREMENT (SUMMARY)	HPES' SOLUTION, METHODOLOGY, AND KEY PROCESSES
Plan	Standardize (4.11.2.1)	• Printers are included in annual engineering and standardization reviews • The County approves standard printers
Plan, Build, Operate	Provide back-end infrastructure (4.11.2.2)	• Printers must be compatible with the County Architecture • Network capacity is engineered to support printers
Plan, Build, Operate	Upon device failure or network failure build in redundancy and failover procedures (4.11.2.3)	• Engineer and maintain for reliability and recovery
Operate	Keep drivers current; maintain firmware (slightly specialized) (4.11.2.4)	• Drivers are maintained via SCCM • Firmware versions are monitored via vendor FAQs and pushes
Plan, Build, Operate	Categorize printers; printers are either standard resource units or in the OIC (4.11.2.8)	• Several classes (monochrome, color, high performance, large format, label and multifunction devices) of network printers are installed • Printers are in Report 44 and the OIC
Build and Operate	Support the User – develop training, tip sheets, update the portal, among others (4.11.2.9)	• User support materials are built by engineering once the printer is selected

STAGE	COMPONENT REQUIREMENT (SUMMARY)	HPES' SOLUTION, METHODOLOGY, AND KEY PROCESSES
Build and Operate	Continuously maintain help desk scripts and support info for technicians (4.11.2.10)	• Printer install and user support materials are built by engineering • Tickets feedback inputs to improvements
Plan, Build, Operate	Leverage existing licenses (4.11.2.11)	• Printer timeline and refresh strategy is maintained to reduce cost of licenses • Strategic negotiation and leverage utilized for license costs
Plan	Make effective standards at the start of each new year (4.11.2.12)	• Printer standards are selected as part of the annual standardization process • Printer vendors brief County and HPES on current products and migration path(s)
Plan and Operate	Supply via the portal a list of consumables (4.11.2.13)	• Consumables list to refreshed annually along with the standards selections • The County can therefore forecast consumables expense and do supply management
Operate	Excluded printers not attached (4.11.2.14)	• Concur
Operate	County shall be responsible for consumables (4.11.2.15)	• Concur
Operate	Maintenance, availability, and break-fix (4.11.2.16)	• In agreement with overall service and break/fix methods • Printer experts are available to assist at all Tiers of support
Plan	Maintain and update annually a timeline/roadmap regarding support to active devices and planned tech refresh (4.11.2.17)	• Printers are part of the overall standards assessment, engineering, test and governance The County approves the standard printers and any OIC printers

Each major activity in the key processes summarized in the table above, has a detailed procedure. An example extract from a detailed printer-specific procedure is below. An example of how HPES supports printers and operates with the County in a multi-vendor environment is our use of Xerox print queue management. Xerox printer provisioning and maintenance is a separate contract between the County and Xerox. We set up the print queues and establish connectivity so they will be in working condition for users.

- Automated Tools – Automated systems and tools involved in proposed solution

The automated systems and tools involved in this part of the framework solution are shown and described in Table 43.

Table 43. HPES value-add to the tools' utilization for The County

TOOL NAME AND VENDOR	DESCRIPTION
Service Manager	• Asset management of printers

TOOL NAME AND VENDOR	DESCRIPTION
Active Directory and Group Policy	• Microsoft environment printer management tools
Vendor- specific print management tools	• Vendor furnished printer management tools and utilities

- Qualifications and Experience – Background and experience in comparable environments

In Table 44, we provide several highlights from our current County contract and similar engagements.

Table 44. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND HOW IT IS RELEVANT TO THE COUNTY
County of San Diego	• We are providing these exact services to The County today: – Six Production and 2 backup print servers supporting approximately 2,700 print queues – The new solution enhances network utilization and increases print performance by separating the print servers between the AT&T POP and the DR POP, redirecting users to the print servers closer to the end user. – Migrate queues per site mapping with more user friendly queue naming.
NASA ACES	• Multi-site. Service-based provisioning of printers and print services, including consumables.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

2.7.1 Offeror Response to End User Services Specific Questions

2.7.1 Your proposed methodology for assessing and mitigating impacts to existing desktop systems and business applications while transitioning to new standard platforms.

Generally, updates to the existing desktop environment, including hardware, core software, and OS, and all other components are organized as follows:

- **Standard Yearly Updates.** These are annual updates to the standard configurations for hardware and Core Software – the total "platform." Concurrently with these updates, hardware equipment that is due for tech refresh will be scheduled so that all changes are made as one event.
- **Ongoing Updates and Refresh.** This activity entails ongoing, incremental, regular updates to approved configurations. Ongoing updates relate primarily to software. We check the hardware inventory annually to determine which machines are eligible for refresh.
- **Ad hoc and Emergency Pushes** – Emergency pushes are event driven. Typically these are defensive security pushes in response to vendor patches to protect the security posture of the standard desktop configuration and/or minor functional updates from the software OEM (versus major version upgrades, which are assessed more thoroughly and are part of the standard yearly update).

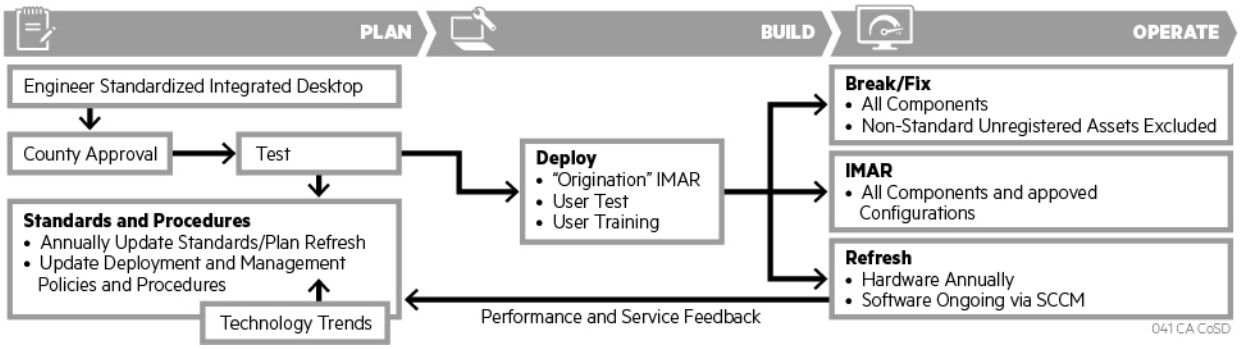
Because this question relates to "mitigating impacts to existing systems while transitioning to new standard platforms" our response focuses on our annual update and refresh activities. In our answers to the first three questions (2.7.1, 2.7.2, and 2.7.3) there is significant overlap in our approach because we use the same core processes and disciplines across all devices and timeframes.

Within the context of the total Plan, Build, and Operate life cycle shown in Figure 60 the answer to this question involves three activities that are vital to the Plan phase:

- Standardization and governance
- Engineering
- Testing

As described above, Enterprise Architecture and Desktop Engineering collaborate on changes to the standards—Desktop Engineering builds and tests those changes and provides updates to the knowledge base and End User Service technicians via documented procedures and cross-training sessions.

Figure 60. End-User Services Framework



Plan Phase activities – standardize and govern, engineer, and test – are vital to transitioning to new service platforms.

Standardization and Governance

The cycle for standards governance and standard desktop configuration updates is annually. As detailed elsewhere, devices are on 3- or 4-year refresh cycles, depending on type.

Standards may be updated based on a County request, HPES' assessment of the technology market, vendor presentations to the County, or other County initiatives. All requests are reviewed and consolidated. HPES' engineering group leads the consolidation and analysis of these requests and brings the County a consolidated list of recommendations, which are presented to the Governance Review Board for approval. Once we have the County's approval, we perform more detailed engineering and testing of the new configurations, as described in the following subsections.

Process to Review and Approve Annual Updates to Standards. Major updates to the standard configurations and core software are made yearly, with a monthly rhythm. The timeline for annual updates to the standard configuration is shown in Table 45.

Table 45. Monthly Flow of Annual Standards

TIMEFRAME (MONTH TO MONTH)	ACTIVITY
Ongoing (January through December)	County performance trend analysis Industry trend monitoring

TIMEFRAME (MONTH TO MONTH)	ACTIVITY
	User needs analysis
October – November	Current industry product assessments by HPES team Vendor briefings to the County and HPES
December	Draft updates to standards Review and approve new standards Update timelines/roadmaps
December	Perform desktop/core software testing and Systems Integration Test (SIT) Perform applications User Acceptance Test (UAT)
January through December	Deploy all tech refresh – annual updates based on device type and user-specific configurations Deploy software refreshes via SCCM

- Governance: Sponsored by the County CIO
- County participants include CIO and staff, and user representatives of each functional organization.
- HPES participants include the COO, Account Chief Technologist, Technology Office Lead, Desktop Services Management, Applications Lead, and appropriate members from those organizations.
- Boards and Review Committees exist for Standards and Catalog management—such as the Configuration Governance Board (CGB) and Catalog Review Board (CRB).

Between the annual cycles and standards governance events, the Technology Office hosts weekly Enterprise Architecture meetings with the County that review new technology trends, vendor roadmaps, and as needed, performance issues in the County environment. These meetings provide ongoing input once a configuration is fielded regarding immediate and/or systemic issues and provide a safety net to the annual engineering and testing cycle.

Engineering

Desktop Engineering is involved before and after standards are set up front with Enterprise Architecture to ingest new requirements, review new and emerging technologies, assess integration compatibility with current and fresh configurations, and recommend new standards. As new standardized configurations are rolled out, Desktop Engineering is involved with resolving Tier 3 tickets and systemic issues. The functions of Desktop Engineering, Integration Engineering, Enterprise Architecture, Applications Management and Operations, as well as Applications Development, IT security, and County business application owners all work together to standardize and test desktop configurations and applications.

Major changes in hardware, operating systems, or other significant architecture upgrades receive more extensive engineering and testing.

Systems Integration and User Acceptance Testing. SIT and UAT testing comes from the Desktop Engineering group using the test lab at the Rancho Bernardo facility. This test lab has multiple device types and configurations to test against to confirm that configurations are ready for deployment. The Desktop Engineer will conduct SIT with the Test Engineer when images are updated and created to make sure the image and software work properly. Test results are peer reviewed and any issues are resolved before production deployment. For major upgrades we will perform full regression testing – user, performance, and security – as part of SIT and UAT.

UAT is performed by both HPES and County users on both types of applications. It is performed when an application is first requested and approved, and when there is a major upgrade to the core software and OS standards.

Overall, this methodology results in a new gold image for new deployments and an upgrade path/procedures for current desktops that may or may not require re-imaging the desktop depending on the scale and scope of the upgrade.

This methodology is governed by current procedures, as shown in Table 46.

Table 46. County Deployment Readiness Procedures

PROCEDURE NUMBER AND NAME
COSD-44 Hardware Add
COSD 48 – Pushed Software Install
COSD- 56 Image Maintenance
COSD – 57 – Image Development
COSD – 65 – End-User Data Profile
COSD – 71 Image Factory Process
COSD 79 – PC Functionality Checklist
COSD 80 – Anti-virus Client Installation
COSD 912 – HW Install Checklist Instructions

Specific Support to Business Applications.

Regarding the business applications part of the question, the first critical item is that we have a user representative for each application. HPES also has an entire Applications organization, led by Mark Roehr, which is responsible for applications and their support.

There are two types of applications:

- Catalog Applications – Catalog applications are typically COTS; they are limited to 440, which is the number we are at now. We monitor the number of applications to control County expenses. We continuously work with the County to help optimize the applications list. As we go forward into the new contract, applications portfolio rationalization and optimization is another area in which HPES business analysts can add value and potentially save costs. Catalog applications do not have backend infrastructure associated with them – they are software packages, typically off-the-shelf. They are installed on the desktop and have no interaction with any other components (i.e., no database or servers it needs to talk to).
- Portfolio Applications - As of January 2016, we had 350 active Portfolio applications. We have had over 400 in the past, but we have retired some over time. Portfolio applications are supported by the HPES applications team and are typically hosted in the data center, on a two-tier or three-tier architecture (thus servers and databases are involved, along with a desktop client most of the time). With Portfolio applications, the project team (more than just desktop engineering, to include the DBA and application SMEs) is involved in SIT before it goes to UAT.

Some portfolio applications (e.g., Kronos) require unique configurations or n-1, n-2 desktop configurations that are not the current standard. We accommodate these needs on a case by case basis. We will work with the County to improve the standardization of these exceptions.

Transformational Opportunities and Updates. Technology is ever-changing and engineering continually seeks to keep the County current with the best available desktop tools, while maximizing usability and security, minimizing risk, and leveraging existing assets.

Desktop hardware makes gains incrementally year over year. The dynamics of Moore's law still apply, even if some the parameters of cost/performance ratios have changed. We do not foresee dramatic changes to the County's desktop hardware in the near term as we have a solid, proven set of configurations in Report 44. We expect year-over-year gains in performance, continuation of a trend toward using more laptops and other mobile devices, and more device management via MDM, and other integration tools.

Desktop software or software architectures are more likely to change. The potential for VDI, Desktop as a Service (DaaS), etc., would require more than the normal annual hardware update process. When fundamental architecture paradigm changes are under consideration, then engineering, business case, and risk management activities must be also considered. An example would be if the County decided to transform to DaaS. This architecture change would have engineering implications on the network, the cloud, and other system components, even if there was no change to the users' functionality. Engineering would assess the pros and cons of alternative architectures, including risks, costs, and security, and would brief leadership in both the County and HPES. We have robust reviews and discussions at the Configuration Governance Board (CGB) and the County must approve before changes are made.

2.7.2 Your proposed methodology for performing Desktop Computing refresh activities as well as maintenance and upgrades to the Desktop Computing Core Software, including the Operating System.

Generally, updates to the existing desktop environment including hardware, core software, and OS; all other components are organized as follows:

- **Standard Yearly Updates.** Annual updates to the standard configurations for hardware and Core SW. Concurrently with these updates, hardware equipment due for tech refresh is scheduled for refresh.
- **Ongoing Updates.** Ongoing incremental, regular updates to approved configurations. Ongoing updates relate primarily to software.
- **Emergency Pushes.** Event-driven, defensive security pushes to protect the security posture of the standard desktop configuration and minor functional updates from the software OEM (versus major version upgrades, which are assessed more thoroughly and are part of the standard yearly update).

Because question 1 above refers to "new standard platforms," our response here focuses on ongoing and emergency update refreshes to the core software, OS, and applications. We focus on this aspect of software refresh but also refer to hardware refresh methodologies and provide additional information.

Refresh is the disciplined and deliberate process most relevant to ongoing maintenance of the configurations. However, as stated in our answers to questions 2.7.1, 2.7.2, and 2.7.3, there is significant overlap in our approach because the disciplines and core processes are the same: identify the reason for the update, assess and engineer the update in accordance with standards, test and confirm the viability of the update, gain County approval (as required depending on the level of the update), update the standard configuration baseline in Reports 43 and 44, plan and deploy the update, test at the desktop to validate that the update was successful, and change logs and databases to document the update and current configuration. Accordingly, we only perform refresh activities which either 1) have passed the configuration control and governance processes to become part of the standard configuration, including

having been assessed for cost/risk/benefit; or 2) are emergency in nature and have been approved through a streamlined process.

Hardware Refresh. With 14,000 desktops and a 3- to 4-year refresh cycle, approximately 4,000 refreshes are required per year to meet the standard. Refresh is an important annual activity and have a group dedicated to refresh, which is a best practice. Our refresh team travels the County working from the refresh list, focusing on one site at a time to minimize disruption.

Based on current hardware refresh data, we know that three quarters of the refresh is for standard PC and laptops—making these procedures highly repeatable and enabling us to automate them to the fullest.

Hardware refresh is discussed in more detail in Section 2.7 and in response to question 2.7.1.

Software Refresh – Software/SCCM.

We use System Center Configuration Manager (SCCM), previously known as SMS, to automate refreshes and updates and manage the overall deployed configuration. SCCM prevents users from installing un-authorized software or authorized software in unauthorized configurations.

The County has more than 15,000 HPES-managed devices (desktops and laptops), for which HPES provides a standard operating system, core software, and catalog and portfolio applications. Over the past 10 years, we have used Microsoft tools to create the image and to distribute software and patches to these devices. Those tools include Active Directory, SMS, and SCCM 2007 for software distribution and device management, along with MDT/OSD for OS imaging. Software refresh includes updates to the OS and applications.

SCCM Upgrade. Under the current contract, we are upgrading to SCCM 2016 to support newer operating systems for managed devices and to take advantage of enhancements in the product, which include improvements to the GUI, monitoring device health, remediating client issues, and deploying SCCM into the Library domain. HPES is building the servers now and plans to have the 2016 framework online by the end of April. The rest of the environment will be built, in production and data migrated by the end of September.

SCCM 2016 core capabilities for the County include:

- Software distribution – by user, by machine; mandatory and optional (self-service)
- Asset intelligence – hardware and software inventory, compliance, application usage tracking
- Hardware and software updates – firmware and security updates
- OS deployment – for workstation only
- Mobile device management - for Windows 8.1 devices (MS Surface Pro 3).

SCCM 2016 will be introduced into the Library environment to maintain currency of and distribute software to the devices on the Library network with the enterprise standard tool.

Using SCCM, non-emergency software refresh will be performed outside core hours, usually at 2:00 a.m.

We have an extensive set of SCCM procedures and related processes; several of the most important procedures are:

- CoSD – 128 New App Release Management Procedures
- CoSD – Microsoft Patch Troubleshooting
- SWM_FIN_Deployment Guide_SCCM

Major software and OS version updates (e.g., from Windows 7 to 10) are considered as changes to the standard configuration and are managed as such. For major OS upgrades, the methodology is more extensive and may include re-imaging the disk. These follow the extensive standards management process described in the response to question 2.7.1.

Requests for Change (RFCs) are used to document the procedures for specific issues. Updates may be applied as a push change or the RFC may remain in the knowledge repository of the Service Desk until a user encounters a problem.

We adhere to the County Microsoft Windows Non Security Updates Process document. We follow overall architecture, desktop, and LAN/WAN security practices, using tools described in Section 2.7.

For security-related updates, the process is very similar. In addition to the steps above, the security office reviews and validates the security updates. Urgent updates are pushed out on an accelerated schedule—either that night, or in the worst case, immediately—in accordance with streamlined emergency approval process.

Approaches, processes, and procedures are governed by the following procedures shown in Table 47.

Table 47. County Update Procedures

PROCEDURE NAME
CoSD DE OS EAD Procedures
CoSD DE Package Engineering Procedure
CoSD New Image Workflow Process
Hardware Image Evaluation
Imaging Quality Assurance Internal Checklist
Microsoft Windows Non-Security Updates

HPES is aware of the County requirements regarding refresh and deployments throughout the year. In 2015, for example, we performed 100 software deployments, 6 of which were enterprise deployments. We expect refresh volumes to continue at historical rates.

Operations and Maintenance of Core Software, including OS.

Desktop Engineering has procedures for maintaining the OS image and core software. On a quarterly basis, new device drivers are tested for items such as printers and network interface cards and added to the OS image. Security and non-security updates are also added quarterly to the OS image to facilitate a faster imaging process. Core software is updated during the year with minor revisions, to address vulnerability issues with the browser, for example. Major revision upgrades of the Core software and OS are addressed via updates of standards that are approved by the County and executed as projects.

The Engineering Acceptance Document (EAD) is an example of a Desktop Engineering process and depicts the integration points and collaboration with other HPES support teams and the County for the OS and specific core County applications, such as MS Office. When a new OS is requested by the County, such as Windows 10, there is a significant number of settings that need to be reviewed that affect performance, security, and user experience. The same is true of MS Office 2013. Below is an outline of the EAD process:

- Create Baseline Comparisons – Desktop Engineering

  - Desktop Engineering is responsible for keeping the baseline tool updated.
  - The baseline tool is used to make policy comparisons of current product/policy settings to new product/policy settings, for example Windows 7 to Windows 10 If there are new features/settings, the Microsoft default is provided.
  - Desktop Engineering provides comparisons to Architecture and Security teams

- Prepare Recommendations – Desktop Engineering, Architecture, and Security teams
  - Validate use cases for new features
  - Compare settings to CoSD and HPES security policies
  - Develop base recommendations for CTO/CISO review.

- Present Recommendations – Architecture, Security, Desktop Engineering
  - Present EAD in Enterprise Architecture meeting for review, covering the major changes between previous product and new product, as well as any new features/settings
  - Discuss impact to the user experience of the proposed settings
  - Obtain CTO concurrence for UAT

- Finalize Recommendations
  - Upon completion of UAT, Architecture, Desktop Engineering and Security review feedback from the County testers, CTO, and CISO. Updates/changes are made as necessary.
  - Present revised EAD in Enterprise Architecture meeting for review and approval to move into production.

2.7.3 Describe your proposed approach to maintain an up-to-date (Core Software) Desktop Computing environment

We discuss our approach to maintain a Core Software Desktop computing environment extensively as a response to the 2.6 Component in the End-User Services Framework.

Generally, updates to the desktop environment, including hardware, core software and OS, and all other components, are organized as:

- **Standard Yearly updates.** These are the annual updates to the standard configurations for hardware and core software. Concurrently with these updates, hardware equipment that is due for tech refresh will be scheduled for refresh.
- **Ongoing Updates.** This is ongoing incremental regular updates to approved configurations. Ongoing updates relates primarily to software.
- **Emergency pushes.** Emergency pushes are event driven. Typically they are defensive security pushes to protect the security posture of the standard desktop configuration and minor functional updates from the software OEM (versus major version upgrades, which are assessed more thoroughly and are part of the standard yearly update).

We interpret this question as focusing on "maintenance," that is, maintaining an up-to-date desktop throughout the year. We have discussed the annual update to the desktop and core software configurations elsewhere. But we note again, and you will read in the answers to 2.7.1, 2.7.2, and 2.7.3, that there is significant overlap of the approach because the core processes and disciplines are the same.

SCCM.

To maintain the core software configuration, we use SCCM (previously SMS) to automate refreshes and updates and manage the overall deployed configuration. In addition, SCCM controls and identifies users installing unauthorized software or authorized software in unauthorized configurations.

The County has more than 15,000 HPES-managed devices (desktops and laptops), for which HP provides a standard operating system, core software, and catalog and portfolio applications. Over the past 10 years, Microsoft tools have been used to create the image and to distribute software and patches to these devices. Those tools include Active Directory, SMS, and SCCM 2007 for software distribution and device management along with MDT/OSD for OS imaging. Software refresh includes updates to the OS and applications.

Under the current contract, we are upgrading to SCCM 2016 to support newer operating systems for managed devices and take advantage of enhancements in the product, which include improvements to the GUI, monitoring device health and remediating client issues, and deploying SCCM into the Library domain. HPES is building the needed servers now, and plans to have the 2016 framework online in April 2016, and the rest of the environment built in production and data migrated by the end of September.

SCCM 2016 core capabilities for the County include:

- Software distribution – by user, by machine; mandatory and optional (self-service)
- Asset intelligence – hardware and software inventory, compliance, application usage tracking
- Hardware and software updates – firmware and security updates
- OS deployment – for workstation only
- Mobile device management - for Windows 8.1 devices (MS Surface Pro 3).

With SCCM 2016 in the Library environment, we can maintain currency of and distribute software to the devices on the Library network with the enterprise standard tool. Using SCCM, non-emergency software refresh is performed outside core hours, usually at 2:00 a.m.

We have a very detailed process documented for using SCCM at the County. We also adhere to the County Microsoft Windows Non Security Updates Process document.

RFCs are for changes to the baseline core software configuration because of issues, new services, etc. They outline the backout plans, testing criteria, etc.

Major software and OS version updates (e.g., from Windows 7 to 10) are considered as changes to the standard configuration and are managed as such. Major upgrades and version changes are managed as part of the annual standards update process and result in changes to Report 43.

For major OS upgrades within the year on a specific desktop, the software refresh methodology is more extensive and may include re-imaging the disk. Whenever possible, we try to bundle major software upgrades concurrently with hardware tech refresh equipment replacement as part of the annual cycle and standards update and tech refresh.

The software distribution process is as follows.

Software Distribution Process

- The County approves the core software standards and configurations.
- Desktop Engineering (DE) posts completed Software Distribution templates to the DE SCCM Production Requests SharePoint site and informs SCCM Ops.
- The SCCM Ops team lead reviews the document for accuracy or any issues.
  - If issues found, he notifies DE and requests update/correction.
  - If no issues found, he sends notification to the SCCM Ops team and applicable desktop engineers that it is approved for production distribution.
- SCCM Ops team member is assigned to perform the setup in the SCCM console.
- SCCM Ops team member sets up the software distribution as specified in the document.

- SCCM Ops sends notification to SCCM Ops team and applicable desktop engineers that setup is complete and includes details of the setup and a link to the advertisement status report for the new advertisement.
- After the advertisement start/mandatory time, SCCM Ops monitors the advertisement status to help identify and correct problems with distribution.

Please note that End-User computer devices are locked so users cannot perform their own installs. .

2.7.4 Describe your proposed approach to dealing with performance or systemic issues on desktops such as Outlook disconnects, unplanned Anti-Virus updates or application performance.

For enterprise-wide systemic issues in the desktop environment, we use ITIL Problem Management to identify the root cause and to drive remediation. Steps include:

- Treat performance and systemic issues as cross-functional problems in that they involve desktop services, engineering, asset management, etc.
- Use data from tools (such as Riverbed, Cascade and APM), users, and tickets.
- Perform analytics; look for patterns and trends.
- Isolate a problem or determine a pattern of the same problem, then attempt to replicate the problem in our test lab so that we can conduct deeper diagnostics.
- Promptly escalate and involve vendor support channels as needed.
- Identify the error and generate RFCs, either to configurations and/or service standards depending on the problem.
- Depending on the nature of the problem and the solution, it may be an emergency push or bundled with a regular release.
- If the root cause of the problem is with the core software configuration, we go through the appropriate engineering and testing process to correct the error, gain the County's approval, and change the standard.

At the deskside level, however, we focus on Incident Management and work to restore service as soon as possible. If we find that there are multiple incidents, or troubling trends, we enlist Problem Management to find the root cause and remediate it.

Deskside break/fix is described in detail in the technical proposal, Section 2.7.

Specific Issues. We are aware how frustrating ongoing and systemic issues can be for both system administrators and individual users. For any issue, we identify it, resolve it, identify the root cause, and then modify standards and/or procedures to prevent the issue from occurring in the future.

To address the specifics in the question:

- Outlook disconnects. This was a major issue for the County, resulting in numerous tickets per month. To address this problem, we established a tiger team with our SMEs on exchange, network, and Microsoft to find the root cause of the issue and put corrective action in place. Since resolving the problem, we have not experienced a recurrence.
- Unplanned anti-virus updates. Symantec released a series of anti-virus patches that caused all desktops in the enterprise to lock up because the CPU and RAM were maxed out. Symantec was engaged and informed us that it had inadvertently released patches to many of its clients ahead of schedule, which caused this issue. We were able to stop this from the server side and within 1 hour of the issue being reported, we had 75% of the environment back up and stable. We have improved our process and tools with Symantec since this event and we have not experienced and do not expect to experience this issue again.

- Application performance. Application issues are usually specific to the application, so it is rare that we identify a common root cause. We maintain a standard set of best practice diagnostic procedures for applications and we engage the application owner promptly when basic troubleshooting techniques do not remedy the problem. To correct these kinds of issues we use the Problem Management process to work through a series of steps that systematically help us correct these issues. To better determine and resolve application performance issues, we will continue to use our Riverbed Cascade analysis software, which allows us to identify performance choke-points within the end-to-end delivery of an application. This, along with the APM tool that is being put in place, which is described in more detail in the Applications M&O section and the data we will be loading into the analytics data warehouse, will make sure that we have all of the data points necessary to determine the true root cause of these issues and to facilitate proactive monitoring.

To recap, we have effective processes in place to identify systemic issues that involve human feedback, trouble ticket data analysis, and system performance data. We have a rigorous process to promptly address the root cause of systemic issues in a reactive sense but acknowledge there is more work to be done to become more proactive in using our reporting and our teams to get ahead of these issues before they become systemic.

To address this, the HPES Operations team, along with AT&T, has started a development process around real time anomaly detection. Currently, we are putting in place automated alarming and event correlation capabilities, with a focus on application and desktop performance. The tools mentioned previously in this section, along with other data center and desktop-based platforms, will enable a layered approach to event triangulation. Combined with the daily stand ups, highlighted in Section 2.8.6, this will help to improve the proactive performance management of services across the enterprise. Currently, the Riverbed Cascade tool is being tuned in a collaborative, cross-framework effort that is already yielding results to establish new monitoring elements, baselines, and thresholds. This is an area that the HPES team and AT&T will dedicate our resources to improve proactively over during the life of the contract, with measured results reported through the operations governance process. As we work through these issues, we will put in place workarounds to keep users fully productive and lessen the impact to them. We have redoubled our efforts to work with the County to fix issues faster and to identify the root cause sooner to make sure that we have the right fix in place for permanent resolution.

2.7.5 Describe your proposed strategy for remote device management

"Remote Device Management" could refer to either Remote Desktop Management or Mobile Device Management. Because of this ambiguity, we provide an answer for each.

Answer 1 – Remote Desktop Management (RDM)

As part of our effort to improve Service Desk processes, we provide a "warm" transfer escalation process between Service Desk and RDM. If support requests cannot be resolved expeditiously by the Service Desk, then the call is escalated to an agent with higher level skills and RDM capability. In some cases, the service desk agent will need to escalate to a higher tier deskside/field team or technical support. Service desk training and detailed documentation outlining the correct escalation path for each type of incident or service request will guide agents to make certain that tickets requiring escalation are routed correctly the first time. We always ask permission from the user before accessing his/her desktop and the user can terminate the remote session at any time.

Remote Desktop Management (RDM). The primary function of the RDM agent is to provide a higher level of technical service, handling problems and issues that the first-tier support was unable to resolve and providing RDM skills to increase first-call resolution and customer satisfaction. Using RDM for remote tool capabilities, agents will remain on the phone with the customer for longer intervals than service desk agents to resolve an incident. RDM agents may interact with network services, software

systems engineering, and/or applications group to restore service and/or identify and correct the core problem. This may require assisting in simulation and re-creation of user problems and recommending system modifications to reduce user problems. Providing seamless support to the customer base, our service desk agents will act as facilitators between customers and other support teams to make certain customer needs are met and tickets are resolved in an expeditious manner.

Remote Desktop Management agents will:

- Take tickets routed to them which require a higher level of technical analysis and will work these tickets to resolution or route to the appropriate Tier 2 technical support group
- Handle problems and issues that the service desk agent is unable to resolve
- Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct a core problem
- Assist in simulation and re-creation of user problems
- Recommend systems modifications to reduce user problems
- Use LogMeIn Rescue as our remote desktop management tool.

RDM typically resolves the user problem before escalation, thereby avoiding the need for deskside support.

Answer 2 – Mobile Device Management

AT&T currently provides comprehensive day-to-day management and life cycle administration of the County's cloud-based AirWatch Enterprise Mobile Device Management solution, which supports more than 3,800 County-owned and BYOD devices. A thorough description of AT&T's MDM Support Services is provided in Section 4.8, MDM Support Services. However, the AirWatch MDM solution includes User Management, Policy Management, Device Configuration Management, and Application and Content Management. The AT&T MDM support team accesses the AirWatch MDM Console and accesses one or more of the following modules for managing a County or BYOD managed device: Dashboard View, Verify Device Enrollment or Registration, Passcode Reset/Unlock, Lock Device, Locate/Find, Send Messages, Run/Create Reports, Add/Delete Users, Device Enrollment (Bulk or Individual), and Wipe. These management capabilities are fully integrated with the County AD infrastructure through the use of the geo-redundant AirWatch Cloud Connectors so that group policies are defined within the AD and implemented via AirWatch. AT&T's Mobile Device Support solution provides multi-platform device management visibility and security controls for industry-leading smartphones and makes certain that enterprise data is secure on both County AND employee-owned BYOD.

While the AirWatch MDM solution focuses on policy and profile management on a mobile device for access to corporate content (e.g., email or internal repositories), the capability for AT&T to remotely control a mobile device through the AirWatch MDM solution is not available. AT&T is committed to working with HPES on a continuing basis to identify remote control technologies for mobile devices, whether through the AirWatch MDM solution or a third party platform.

2.7.6 Describe your proposed methodology for supporting County managed mobile devices.

For County-managed mobile devices (e.g., handheld devices, smartphones, tablets, and other county retained mobile assets), the methodology in technical proposal Section 2.7 for MDM applies. From a business management standpoint, any device that is "County managed" and outside the scope of RU fixed price support would require T&M support and a Non-Discretionary Work Request (NDWR) to bill break/fix work related to PAIDs, perform preventive maintenance, hot fixes, small project type work, etc. For example, if a user wants support on its application, an NDWR is required.

The County's current MDM solution is focused on security and policy enforcement. We can mitigate against risks such as device loss, data loss or breach, and exposure to malware by using inherent capabilities of the Airwatch client. As use cases continue to expand, these security features remain critical to maintaining a stable enterprise mobility solution.

Increasingly, County departments are developing and using business-unit-specific mobile applications to support their unique needs. As these applications become more widespread, AT&T will enable secure, VPN-based interaction with enterprise data using one of two methods. First, using the Pulse Secure mobile client, applications can be launched establishing an encrypted connection to the enterprise via the same SSL VPN solution used for enterprise computing. Second, applications can be developed with onboard programing to use "per-application VPN," a capability inherent to the Airwatch solution in which a secure tunnel is established from the application to the enterprise via the Airwatch Mobile Access Gateways. Both of these solutions are available and viable today, and provide the County with the necessary security between the mobile device and the enterprise.

County businesses are also seeking ways to interact with enterprise content and services from their mobile devices. AT&T recognizes the business value of these capabilities and has defined a support model to provide new content and collaboration features for End-Users. In the near term, AT&T will be enabling Airwatch managed content and collaboration features, using the Airwatch Secure Content Locker tool. This tool will allow for direct access, encrypted access to enterprise data, leveraging containerization capabilities to prevent data transfer to external sources. In addition to these capabilities, secure access to web-based services such as SharePoint will also be enabled, further enhancing the business value of the service.

As the mobility roadmap projects outward, and converges further into the enterprise, content management will move towards a standard solution that will be enabled by the overarching support provided by the Airwatch MDM solution. This solution could involve more specific data loss prevention policy, coupled with more open yet secure access to County data using more traditional VPN technology as a standard. Overall, AT&T's goal is to provide a seamless user experience for any County mobile user from any device, while providing the appropriate level of security through well-thought-out policy management.

A significant increase in the adoption and deployment of smartphones and tablets has occurred due to a major mobilization of the County's workforce. The business drivers causing this shift in the way employees work will continue to create demand for increased capabilities and functionality in mobile devices over the term of the new contract. To meet this need, our service offering is expanding not just in the functionality it provides, but also in the support it can offer to the County mobile users.

AT&T's proposal for enhanced support improves upon its MDM management capability to meet the broader needs of the County's mobile user. AT&T will now be the single provider of comprehensive support for County-owned and BYOD mobile devices that are configured for business use. AT&T will now act as a central point of contact for all device and multi-carrier mobility issues, using the HPES Help Desk process as the conduit. This solution will include assistance with device and operating system issues, as well as a "warm transfer" process for County users for issues requiring wireless carrier intervention. AT&T's fully Managed Mobile Device Support Service solution will also continue to provide the same comprehensive support for the daily, ongoing configuration and life cycle administration of the Airwatch MDM platform.

AT&T's full service, comprehensive management capability will allow County department IT staff to spend less time assisting users with basic troubleshooting and familiarity issues with their devices, enabling them to focus more on the business. Also, this solution sees to it that the County departments maintain the flexibility to choose the carrier that best meets the needs of their business.

AT&T's Mobility solution meets the requirements of the County today and into the future. Its MDM platform, AirWatch, is the market leader because of the rich feature set, ease and flexibility of use, and continued enhancements available through a cloud hosted solution. AT&T's service directly supports the security of mobile devices, County data, and applications in an increasingly complex environment and will continue to converge capabilities across the enterprise, enabling more and more functionality to the mobile user.

In summary, AT&T's mobility support solution enables the highest degree of security and functionality, while providing a single point of contact for all mobility needs, simplifying the user interaction and improving mobile user productivity.

2.7.7 Describe your proposed approach to engineering desktop software, and to constantly improve quality and timeliness of applications and software package delivery to End-Users.

HPES's approach is grounded in our integrated cross-functional framework delivery model. Much of the information that responds to this question is provided in our responses to questions 2 and 3, and also in the technical section for Desktop Engineering and Core Software Management.

We will organize our response around:

- Service to the user
- Approach to engineering
- Continuous improvement
- Quality and timeliness of delivery.

Service to the User.

The user will be involved and, more importantly, will have a voice and authority during each phase of our approach.

Plan

- A user can initiate a request via the Service Portal for new software or applications or support to existing software or applications
- Users, Group IT Managers, CTO, and HPES Applications team representatives are involved in the annual standards refresh along with Enterprise Architecture and Desktop Engineering
- Users, Group IT Manager, CTO and HPES Applications team representatives are involved in the weekly Enterprise Architecture meetings with Desktop Engineering
- Users help specify and conduct user acceptance testing (UAT)
- Applications must be tested both by HPES (first) and the sponsoring user

Build

- User manuals, FAQs, and other supporting reference material are configured and deployed.
- User feedback from prior similar deployments is incorporated

Operate

- User receives an introduction deskside to new equipment and software
- Various types of user training are available depending on the nature of the software and applications
- User service is always available via the service desk

Desktop Engineering

Desktop Engineering has been described throughout this section, specifically in 2.7.1, 2.7.2 and 2.7.3. To summarize, most of the applications in use by the County are COTS or were developed by other vendors. Requests for packaging software for the desktop are made through catalog requests or project requests from the County. As such, Desktop Engineering creates the installation package, tests it in the engineering lab, peer reviews it, and provides it to the client to conduct UAT, in the case of a catalog request; the HPES Applications team for testing, in the case of project/portfolio requests. Upon successful Applications team testing, client UAT will be conducted. When client approval has been obtained, Desktop Engineering submits the request to End-User Services – SCCM Ops for production deployment.

Performance Monitoring – We monitor the performance of the applications and hardware devices as part of the overall enterprise. When there is a reason for deep applications or any kind of additional performance monitoring, we perform troubleshooting and analysis using the tools and teams that we discussed previously in this section. The addition of the analytics data warehouse that we will be putting in place as described earlier in this section will pull together the complete view of the information and data that we have within our systems. This will ensure we are not only resolving the issues reported as quickly as possible but are putting the appropriate measures in place to become more proactive and to assess and improve the environment and hardware as needed for continuous improvement..

Performance Tuning - When applications need tuning, we work cooperatively with the application vendor and the HPES Applications team.

Continuous Improvement

Continuous Service Improvement (CSI) derives from process quality issues that can affect service delivery and is measured by Service Levels. When MASLs identify a process quality issue, we implement CSI following the standard Deming Cycle (Plan/Do/Check/Act) (see Figure 61). We will on a continual basis seek to improve end-user services by identifying improvement areas, planning and implementing remediation's, and measuring the change in our quality metrics.

Figure 61. Continual Improvement

As an example of tuning and improving our configurations and service aligned to the department's business needs, we have conducted applications rationalization in the last several years. At this point we are confident that each department has preferred vendors and applications that meet its additional special requirements.

Quality and timeliness of delivery

The quality of desktop performance is constantly assessed at many levels. Users need optimal system availability and performance so that they can do their jobs for the County all day, every day.

Quality of Applications. Quality of applications and their hosting is tested as the application is approved for the standard configuration or OIPC. In addition to HPES-performed SIT and UAT, the hosted application is tested by the sponsoring user, who knows the application best and provides his/her own UAT. Finally, the applications in the configurations are tested by service technicians when an IMAR or refresh action warrants. Testing has been explained in depth in the main section of the proposal response.

Timeliness of Software Package Delivery.

There are several potential "pinch points" in the processes which can delay the timeliness of applications support. We will proactively work throughout the process to facilitate the speed with which users can obtain new applications and the speed with which they can supported. Applications go through the Plan, Build, and Operate process.

Plan.

The speed at which a new application request can be approved is related to the quality of the application, the urgency of the request, and the complexity of the application in terms of how it integrates into the standard architecture. We will work closely with the County during each step so each application request is prioritized correctly. We will use the GR, CRB, and weekly Enterprise Architecture review meetings as forums to achieve this. And County leadership can always ask for accelerated approval as a special project under DCMR. The County must approve requests for new applications and these decisions are made once a week. Applications must be tested both by HPES (first) and the sponsoring user. Some packages require legacy configuration of the standard desktop. HPES accommodates all applications, but one way to get more timely service is to port as many applications as possible to the current service of the standard desktop.

Build.

Once an application is approved, during the Build phase, delays usually occur only if there are engineering issues related to installing the application in the standard configuration. We will address these issues on a case by case basis and work cooperatively with the application owner. The County has the weekly architecture review to help prioritize as well. Client UAT is critical to this process. Availability and scheduling of end users for testing of the catalog and portfolio requests facilitates timely deployments and joint success for the County and HPES.

Operate.

As applications are released as approved and are part of OICP, all standard procedures apply, which makes applications and Core software delivery (install and operate) just as timely as other core standard elements of the configuration. There are approximately 840 applications. Applications operational issues are resolved at the highest possible tier, but some applications are specialized and complex. Applications escalation is a Tier 3 item.

Executive Summary - End-User Services Framework

Include cross-framework/component integration, competitive differentiators, and County benefits to your proposed solution.

Summary

As shown in Section 2.7, we do everything required in the Exhibit LL SOW. We deliver solid End-User Services today that are consistently meeting all MASLs. We plan a straightforward transition to the new contract in the End-User Services framework because operations are already stable and efficient using current architectures, tools, strategies, methodologies, and approaches. In addition, we meet all the technical evaluation criteria in this framework and its laterally evaluated components stated in the front of the RFP:

Evaluation Factor 1 – "Describes solutions and identifies any issues with how each requirements in the statement of work will be achieved."

HPES' solution is fully described in Section 2.7 and we are confident we can meet County requirements.

Evaluation Factor 2 – "Clearly demonstrates how implementation of the proposed approach will deliver timely, standard, stable, reliable, secure, flexible, responsive, compliant, and cost effective services to meet the needs of the county and its stakeholders."

We have highlighted throughout the section our interactions with and the benefits to the End-Users. Our deskside technicians are aware of several important factors:

- Customer service in all dimensions – technical timeliness and accuracy as well as a professional experience with a friendly, personal touch – is the essence of every interaction. As one of our leaders reminds us: "The excellent work we do today, earns us the opportunity to serve the County tomorrow."
- At the deskside, users may be frustrated with their equipment. Therefore, we remind our service technicians to respect the user's situation and fix the equipment as promptly as possible—in a friendly and courteous manner. The human touch is just as important in keeping the technology running and achieving high levels of customer satisfaction.

Evaluation Factor 3 – "Commits to proven processes and procedures that ensure high quality performance."

HPES commits to ensuring high-quality performance, to continuous improvement, and to evolve our services over time to leverage emerging technologies and meet new user requirements.

- HPES is the well-performing incumbent today, meeting all SLAs in the End-User Services framework while achieving nearly 50% of 5-star ratings in customer satisfaction.
- This is not luck. HPES is following documented and proven standards and procedures to achieve this performance. As documented in this section of the proposal, we have dozens of procedures that apply directly or indirectly to End-User Services, as documented elsewhere in this section of the proposal.
- We have a very low-risk transition in End-User Services because there are no major upgrades to be performed in desktop configurations or support. HPES improved performance and further mitigated performance risk last year when we upgraded Network Print Services and migrated to Service Manager in 2016.
- We are ready to support transformation activities, such as VDI, when approved by the County.

Evaluation Factor 4 – "Commits to and demonstrates the ability to assist the County in upgrading its application portfolio and to provide guidance and leadership in Business Process Re-engineering efforts."

Support to Business Process Reengineering (BPR) involves more than end-user service and maintenance in accordance with the standard desktop and core software configurations. This requirement is primarily met by the program office, engineering, cross-functional, and applications frameworks. HPES stands ready to identify and support BPR opportunities. Within the context of end-user services, we will provide metrics and trend data/analysis that feeds overall architecture and business requirements fulfillment efforts. This utilization and reliability and service data will help feed ongoing engineering analysis, trend analysis, and County mission-needs assessments.

As an example, by introducing applications virtualization, we add flexibility to host legacy applications going forward. In the cross-functional section, we discuss our business analysis services, EDGE methodology, and Business Analysis Center (BAC). We are excited that this requirement gives us the ability to support business process reengineering and expands and enriches the way in which we can work with the County to achieve its mission.

EXPERIENCE CALLOUT: For the Navy Fleet Rating Identification Engine (Fleet RIDE), Navy hired HPES to lead business process reengineering and obtain consensus on new processes with the Reclassification Classifiers. HPES accomplished this through functional process improvement workshops to capture both process changes and Fleet RIDE functional requirements. This work included fit/gap

analysis, blueprinting, and pilot to confirm the effectiveness of the to-be business process model. This allowed the Navy to retire the legacy Perform to Serve (PTS) system, while improving efficiency and effectiveness.

Table 48 summarizes HPES' differentiators and value to the County in End-User Services.

Table 48. End-User Service Highlights

SOLUTION HIGHLIGHTS AND KEY ELEMENTS	DIFFERENTIATOR(S)	COUNTY BENEFITS
Over 100 County procedures document and guide our delivery today in this framework and require little or no change We are functionally organized Onsite technicians dedicated where end-user populations are highest and/or most critical Framework model is flexible to surge and make improvements, (e.g., increasing RDM) Framework is in place today and functioning well in service to the user…largest technician teams organized for break/fix, refresh, IMAR	• HPES has demonstrated the ability to deliver County-specific service • HPES Service Manager provides the overall framework integration for smooth ticket management and service between tiers • HPES' processes support the County with standardization, yet flex to accommodate more than 800 different applications	• Lowest transition risk • Low cost while meeting user expectations, needs, and service levels • IT infrastructure provides the foundation for future transformation and continued cost savings

We will deliver a Client focused – low risk – high performing Desktop Services framework.

Finally, the County knows that HPES' service model works well for the County. We have 10 years of experience on the team, and we have refined this model over the last 5 years as prime contractor. Our Tier 2 technicians provide the best modern deskside service and bring a level of customer knowledge and support that cannot be delivered from a virtual environment by generic technicians. The County will benefit from staying the course and retaining HPES' End-User Services.

2.8 Network Services Framework

Executive Overview

The County's network is the cornerstone of its IT strategy. With a focus on steady, progressive change, the County has increased network reliability and reduced single points of failure. This resilient architecture will serve as the foundation for the County's future network: a cloud-based, virtualized environment that offers rapid provisioning, near-real-time changes, and differentiated services based on user roles. The HPES network team has the knowledge and vision to help the County achieve this goal.

Experienced Governance. We provide local staff with an average of 9 years of experience supporting the County. This team has established the relationships that foster open and innovative collaboration. Our approach focuses on close collaboration with the County Technology Office and the HPES architecture team, where technical leadership meets weekly to discuss strategic objectives, technology, and industry drivers for new solutions. Our team helped evaluate, test, and implement 68 continuous improvement initiatives in the last 5 years alone, and we have many more planned for the County's future roadmap.

Approach to Progressive Transformation. We have adopted a "Start Fast" approach that allows experimental and rapid evaluation of technology many times in a production environment. This approach has proven extremely effective in driving continuous improvement across the enterprise. As we evaluate and test new technologies this iterative practice makes certain that roadmaps remain agile. We save time, drive change faster, and identify fatal flaws before we introduce solutions. With this approach we can offer more capabilities, functionality, and capacity—often with no additional costs.

The Future of the County Network. Our approach to progressive transformation will continue to position the County as a leader in its adoption of IT as an enabler to the enterprise. The County will benefit from our evolution toward software-defined networking (SDN) and network functions virtualization (NFV). This new approach to network management and control can help the County simplify operations, reduce capital expenditures, and improve performance.

We have already rolled out several virtualized services, and we have more planned in the coming years. To position the County for cloud-based, software-defined networking, we recommend the following:

- AT&T NetBond to provide highly secure, performance-assured, and cloud-to-enterprise peering.
- Migrate the County's existing Ethernet and T1 sites to AT&T Switched Ethernet with Network on Demand, which will allow near-real-time bandwidth provisioning.
- Pilot universal CPE (uCPE), the next step in the SDN evolution. uCPE is a standardized device that acts a virtual machine for network functions. By eliminating specialized devices, uCPE can significantly reduce complexity and capital costs.

Our investment in NFV, SDN, and cloud technologies will change the approach to network management, security, and cross-functional operations; as a result, the County can greatly improve processes and reduce costs. Your existing support team is committed to helping the County put these new technologies to work. We have demonstrated our dedication to ongoing transformation throughout our future plans for our network and services, and they tightly align with the County's vision. By selecting our team the County can eliminate the risks of transition to a new network and continue to focus on improving its IT infrastructure.

Data Network Services (Sched. 4.3, Section 5.5)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Working closely with the County, our team plans transformational activities (including contractually obligated refresh, upgrades, and strategic initiatives) that build on our track record of operational and service excellence. Our focus on continuous improvement and architectural strategy enable County business to grow in key areas according to jointly developed strategic roadmaps.

Collaborative Approach

As the County network becomes ubiquitous and available to users and their devices anywhere, the solutions we deliver must focus on continuously improving performance, security, and accessibility while reducing the probability of outages. Through involvement in weekly CTO architecture sessions, as well as participation with the Enterprise Architecture (EA) governance process, we propose new technologies that have been evaluated and measured against County strategy and business requirements. This continual dialogue with the County, along with our broad industry knowledge of network solutions and their impact on adjacent technical disciplines, allows our team to successfully propose and implement emerging technologies within or even before the agreed-upon technology refresh cycles. This approach allows the County to quickly realize the benefits of new technologies. This ongoing interaction also facilitates the standardization of hardware and software deployed by our team as our solutions receive initial approval from the Enterprise Architecture Forum and subsequently from the Change Review Control Board prior to transformation.

These collaborative efforts between the County and our team have resulted in a core network configuration that has evolved over the current Contract cycle to provide a consolidated, disaster recovery-ready, high-availability, and high-performing infrastructure. A current view of the overall network is shown in Figure 62.

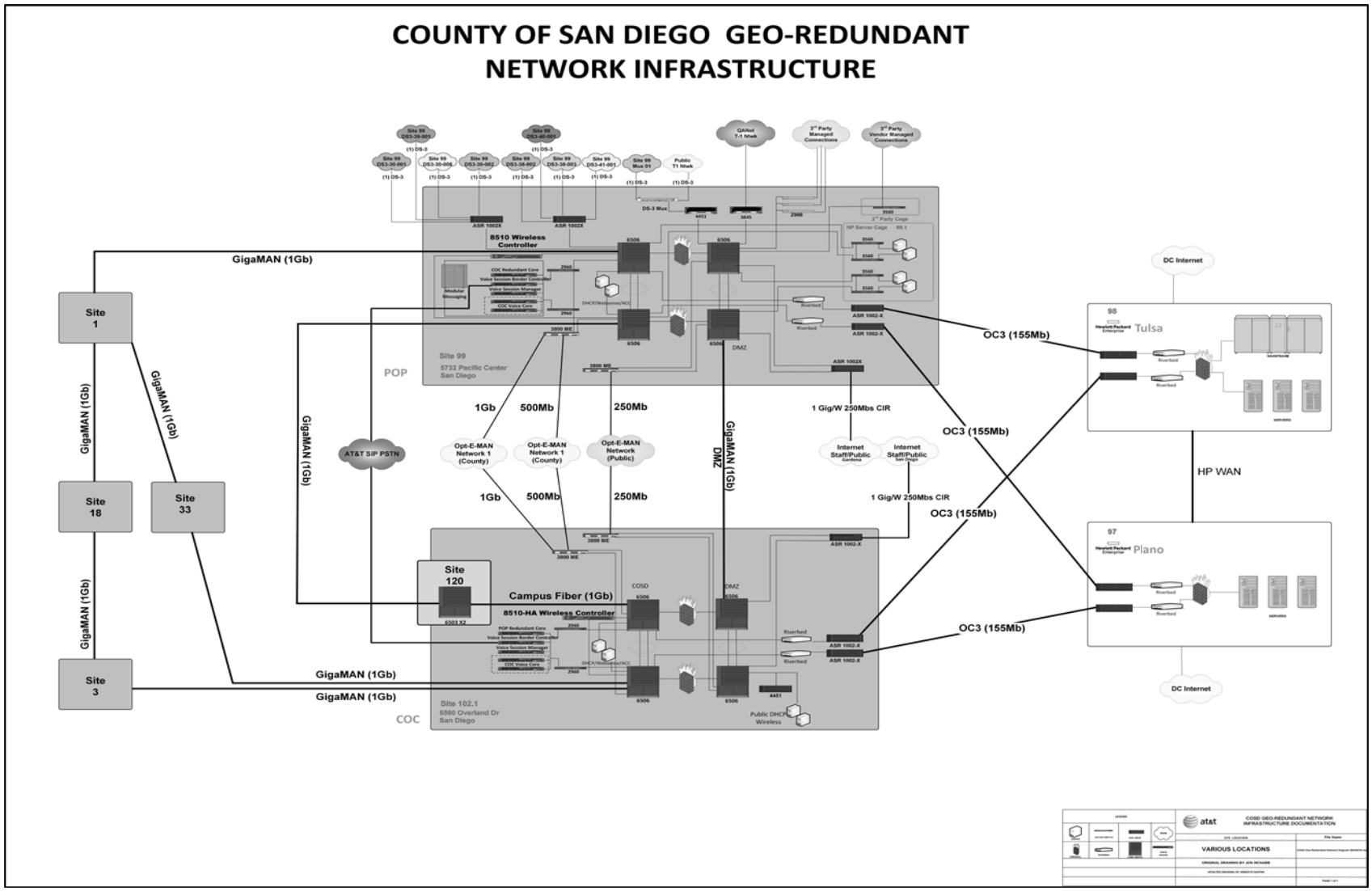
Upon activation of our approved solutions, we employ several automated tools to maintain an accurate and up-to-date inventory of all hardware and software supporting data network services. In addition, we use automated tools to continuously monitor the provisioned services from an operational and bandwidth utilization perspective, as well as provide valuable insights into traffic patterns and application functionality.

Monitoring and Management Approach

From an operational view, our capacity and performance management tools continuously measure and report on delay, packet loss, retransmissions, bandwidth use, and service interruptions. In the case of an outage or degraded services defined by specific thresholds, automated alerts and page-outs are sent to our local, dedicated team members who respond to resolve incidents within Service Level Agreement (SLA)-specified parameters. During normal business hours (6 a.m. – 6 p.m.), the engineering and help desk teams monitor operational status using CA Spectrum and actively respond to alerts. After hours, our team uses the automated notification features within the tool to provide the necessary alerts that trigger incident response activities within stipulated SLA parameters (24x7x365).

As part of our prompt restoration services, we report incident response activities to the County using the centralized HPES Ticketing System. Additionally, on P1 and P2 outages, as well as upon County request, we will develop root cause analysis documentation and submit it for review. Incident reporting also includes a proactive response to performance or capacity issues, and our reporting clearly identifies the nature of the incident or degraded performance and the steps taken to resolve the issue.

Figure 62. County Network – Current View



The County's geo-redundant infrastructure has been continually improved and expanded, increasing redundancy and improving network performance.

Our network performance management also uses CA Spectrum to provide monitoring. One component of CA Spectrum is CA eHealth, which we use to perform trend analysis based on historical measurements as well as current indicators to model, optimize, plan, and report on network services. This tool allows us to meet the County's requirements for speed, reliability, capacity, and quality. CA eHealth also provides real-time and predictive performance analysis capabilities, enabling identification and provisioning of increased bandwidth capacity prior to reaching user performance issues on the intranet or Internet.

Although CA Spectrum provides passive network monitoring and measurement techniques, Cascade Pilot and Cascade Shark allow active capture, measurement, and analysis of network and application traffic in support of anomaly detection and forensics. Our team uses these deep packet analysis tools to trend application network performance—establishing thresholds that can be alarmed, correlated, and compared to baselines, enabling a proactive approach to identifying application or desktop issues. Additional network-based tools enable a layered approach to trend analysis and event correlation, including Security-based tools such as Palo Alto's Panorama (packet capture and analysis, application identification, traffic volume identification, malware detection, and threat identification); Wireless tools such as Aruba's Airwave (Wireless capacity/ performance); and Voice tools such as Nectar (quality of service [QoS], mean opinion score [MOS], jitter/latency measurement, and round-trip time [RTT] analysis). As we continue to evolve our approach to real-time anomaly detection, new tools and processes will be evaluated and proposed—improving our capability to support adjacent frameworks in identifying enterprise anomalies that would otherwise go unnoticed until an end user reports a symptom. Proposed changes in the processes and personnel using and evaluating data from these tools can be found in Section 2.8.6.

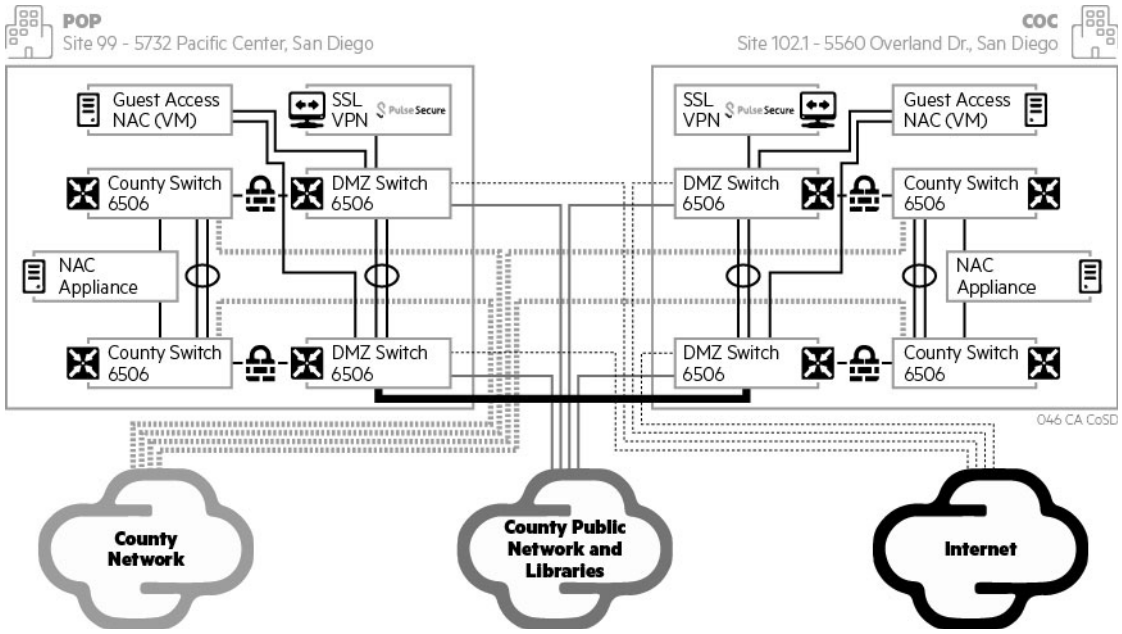
Continuous Improvement

Our team develops and maintains tactical and strategic roadmaps that define solutions to business needs in line with industry advancements and County strategy. As an example, although GigaMAN and OPT-E-MAN have been the predominant WAN transport technologies over the past 9 years and fully meet current SLA parameters, our team has recently recommended and received approval to begin implementing AT&T Switched Ethernet with Network on Demand (ASE/NoD) WAN connectivity as a new site standard. The solution provides improved performance characteristics along with improved packet delivery rates and network availability. An additional ASE/NoD feature uses software-defined network technology to allow our local staff to dynamically adjust bandwidth at a site within a 15-minute window based on business need; historically, this adjustment would take more than a week to provision. Additionally, our team is collaborating with the County Enterprise Architecture Forum to identify and remove single points of failure (SPOFs) within the current infrastructure. To date, our teams have removed numerous SPOFs within the network core, providing redundancy and connectivity to data center, network, and cloud-based resources for remote sites through two dynamically available, geo-redundant points of presence. We will use this centralized design in our proposal as we develop plans to eliminate single homed T1 sites from the environment.

Our proposed network is designed to provide maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest security and service levels. Acting as an "enabler to the enterprise," our proposed network will allow any device—managed or unmanaged—to be evaluated, authenticated, and allowed policy-based access. This next generation network will transform the enterprise by reducing cost and increasing flexibility while improving security and service levels. This new technology will be expanded in the new term, replacing Opt-E-MAN circuits as well as T1 circuits where possible. We discuss this migration approach in more detail in Section 2.12 of our network transformation response.

Figure 63 shows the future state of the centralized, geo-redundant, high-availability network core.

Figure 63. County Network – Future State



County network transformation (future state topology) takes advantage of AT&T's latest software defined network and cloud-based solutions, simplifying the network topology while improving performance, availability, and security.

Transformation Opportunities

Currently, the County is evaluating cloud-based services to provide cost-effective ways of delivering services to employees and constituents. Our team has already identified the transformations required to receive the full benefits of cloud architecture. We are proposing an AT&T NetBond solution that extends connectivity using a Multiprotocol Label Switching (MPLS) network into County-selected third-party vendors. The NetBond solution will provide a secure, performance-assured interface to the cloud, while offloading the Internet Service Providers (ISPs) and dedicating bandwidth to the services. Additionally, our proposed solution facilitates fully integrated and centralized connection management functionality and supports third-party cloud services with our contractual service levels.

The foundation of this service will be deployed in a geo-redundant manner, using AT&T Virtual Private Network (AVPN) MPLS circuits; it is included in the Data Network Services and is priced in Exhibit 16.1.1. Future implementations of NetBond services (proposed as a resource unit (RU) on a bandwidth basis, listed in Exhibit 16.1.2) will use this transport connectivity to create the peer-to-peer connection with the selected cloud provider (cloud provider costs may apply). The intent in proposing a NetBond RU is to provide the County with predictability in estimating the County side costs of migrating services to the cloud, facilitating evaluation of the business decision.

In support of the transition of Exchange to the O365 cloud, and in line with Microsoft's recommendation Contractor will ensure adequate bandwidth is provisioned on the geo-redundant Internet ISP's to allow access to O365 services. As an option for isolating this service away from the ISP, Contractor will also offer optional NetBond functionality in a peering arrangement with Microsoft's Azure Express Route product. The solution will be evaluated as part of the design effort and will be offered as an optional service, and priced as a separate RU that combines the NetBond RU (highlighted in Exhibit16.1.2) with the Express Route costs to complete the connectivity model for the service.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The network framework team maintains infrastructure in County facilities and works closely with the County Technology Office and the Department of General Services to support accessibility and security.

The local life cycle management (LCM) team consists of dedicated, full-time resources—many of whom have worked on the County's network for a decade or more. Our primary location will continue to be our existing operations facility at Trade Street. All LCM technical, operations, and project management personnel work out of this location. All network services framework components rely on the use of the AT&T point of presence (POP) and the County Operations Center (COC). These two geo-redundant sites are the core locations holding the centralized communications equipment, appliances, and transport capabilities that securely enable feature-rich capabilities to every business area within the County.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Our team will apply the following key methodologies in our proposed solution:

- Iterative and bi-modal approaches to solution evaluation: "Start fast," evaluate options, and align solutions to County business needs and long-term strategies; establish proofs of concept, all prior to discussion on cost/price.
- Weekly architecture team collaboration sessions allow a continual transformative approach to be maintained across the entire network framework.
- Weekly Enterprise Architecture Reviews enable cross-framework dialog so that adjacent requirements are understood and delivered.
- We employ ongoing, discipline-specific technical roadmap development.
- HPES uses a structured refresh process, at 4 years, for core routing infrastructure; and 5 years for LAN switching infrastructure. This approach will be continually reviewed with the County, making certain that the refresh activities will bring the greatest value to the County, with options for deferral provided while taking service level performance into account.

- Automated Tools – Automated systems and tools involved in proposed solution

We use the automated tools shown in Table 49 for Network Services.

Table 49. Network Services Automated Tools

DATA SERVICES AUTOMATED TOOLS	USE
CA eHealth	Performs capacity, performance, and trend analytics for circuits
CA Spectrum	Monitors all network equipment—routers, switches, wireless access point (WAP) controllers, and WAPs—and provides alerts/alarms based on predefined parameters
Cascade Shark	Performs NetFlow data capture for subsequent troubleshooting and in-depth packet analysis by Cascade Pilot
Cascade Pilot	Performs in-depth network packet analysis
SMARTnet Total Care	Discovers and reports on all Cisco equipment and maintains the database of all Cisco equipment

DATA SERVICES AUTOMATED TOOLS	USE
Airwave	Provides inventory and control of wireless access points and controllers
Cisco Prime Infrastructure	Provides Cisco equipment configuration management and control; backs up equipment configurations and manages licenses

HPES continually evaluates the automated toolsets used in managing data network services, making recommendations to change and improve services through the Enterprise Architecture Forum, as well as ultimately implementing the solutions through approval from the Change Review Control Board.

- Qualifications and Experience – Background and experience in comparable environments

Our team's local staff have an intimate understanding of the network, with an average experience of nine (9) years acting as implementers of transformation activities for the County highlighted by

- Field resources have extensive experience accessing and conducting work in County facilities, while maintaining local site contract relationships
- Network framework operations, project management, and engineering staff work directly with County departments and have learned County processes
- Very low transition complexity due to incumbent performance, as well as local and knowledgeable staff
- More than 34 distinct technical certifications, including Certified Information Systems Security Professional (CISSP), Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), Cisco Certified Design Associate (CCDA), Certified Wireless Network Administrator (CWNA), and others

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Remote Access Services (Sched. 4.3, Section 5.6)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

County employees are increasing their use of mobile devices to conduct County business, and they often use their laptops to access County resources from remote locations. In addition, the County provides third parties access to some resources. These users require secure, reliable access to County IT domains:

- County credentialed users may operate outside the domain, but they need direct access to domain resources.
- Third-party vendors outside the physical and logical domain must gain controlled access to designated domain resources.

To support these evolving needs, we will maintain our scalable and secure remote access solution to provide the necessary breadth and depth of functionality. In close coordination with the County, HPES has implemented a suite of remote access services via Secure Socket Layer (SSL) connections to satisfy

these evolving requirements through numerous transformation initiatives. Because our SMEs have extensive knowledge of the County's environment, objectives, and security requirements, we are able to quickly leverage transformational solutions to benefit the County. These low-risk implementations emphasize minimal operational disruption and demonstrate our commitment to continual service improvement.

Our experienced, on-site dedicated staff members maintain safe, reliable, and secure sessions allowing user-role appropriate access to County resources as dictated by County policies and enforced through the use of groups established within Active Directory (AD). This solution set offers an inherent advantage by leveraging the existing AD capabilities already being paid for by the County. This solution precludes the need to logically connect a disparate system to AD. Instead, we use the features already purchased and available. This approach maximizes your existing investment and reduces your total cost of ownership.

To maintain the security and privacy of County resources, we establish specific Active Directory group profiles that allow users and capabilities to be directly tied together through specific rule sets for each user within the group. Thereafter, Computer Services Registration Form (CSRF) tickets provide the direction and authorization needed to assign specific users into their designated profiles. As a result of their specific group membership, users are allowed access to a predefined set of resources and precluded from accessing other resources. In this manner, our staff enforces County-directed policies and presently supports more than 2,600 remote users within three distinct group profiles.

Our remote access services will be provided via two independent resource units, Network Persistent VPN, (Virtual Private Network Level 1) and Application Persistent VPN (Virtual Private Network Level 2). These two resource units may be subscribed to stand-alone or in combination and will apply to the infrastructure, maintenance and support of the hardware and software behind the remote access technology. Base access costs are recovered through the Network Access Wired/Wireless RU and will apply to all County domain registered users.

PulseSecure SSL VPN – Network Persistent VPN (Virtual Private Network Level 1)

Due to the ever-increasing importance of remote access services, we have activated geo-redundant remote access gateways from the County Operations Center and the AT&T POP. This solution uses PulseSecure PSA7000 appliances in the two POPs in conjunction with PulseSecure software loaded on the laptops to facilitate SSL virtual private network (VPN) access into the County domain. Our solution is proven to work with wired and wireless configurations.

This network-persistent solution eliminates a potential SPOF related to hardware or link failure by detecting a failure in one PSA7000 and automatically switching to the alternate without user intervention. Currently, all SPOFs related to remote access have been removed. We will continue to evaluate any changes to the environment to identify potential single point of failures, and we will work with the County to eliminate them.

Although this solution presently supports more than 2,600 remote users in three group profiles, there is capacity and flexibility to expand further, as needed, to support additional users and profiles. This scalable solution supports three profiles—SSLVPN1_D, SSLVPN1_DRW, and SSLVPN1_DRWF. Network access control is achieved through a feature known as host checking; the remote host is verified as being either a County-owned device or a non-County device and granted domain access as appropriate. For those with full domain access this solution provides further granular control by restricting or allowing the use of additional features. For instance, two of the user groups may use Remote Desktop Protocol (RDP) to gain logical access to their work computers. Our proposed solution has the adaptability and flexibility to meet the County's requirements today and into the next service Contract. Our geo-redundant solution is depicted in Figure 64.

Figure 64

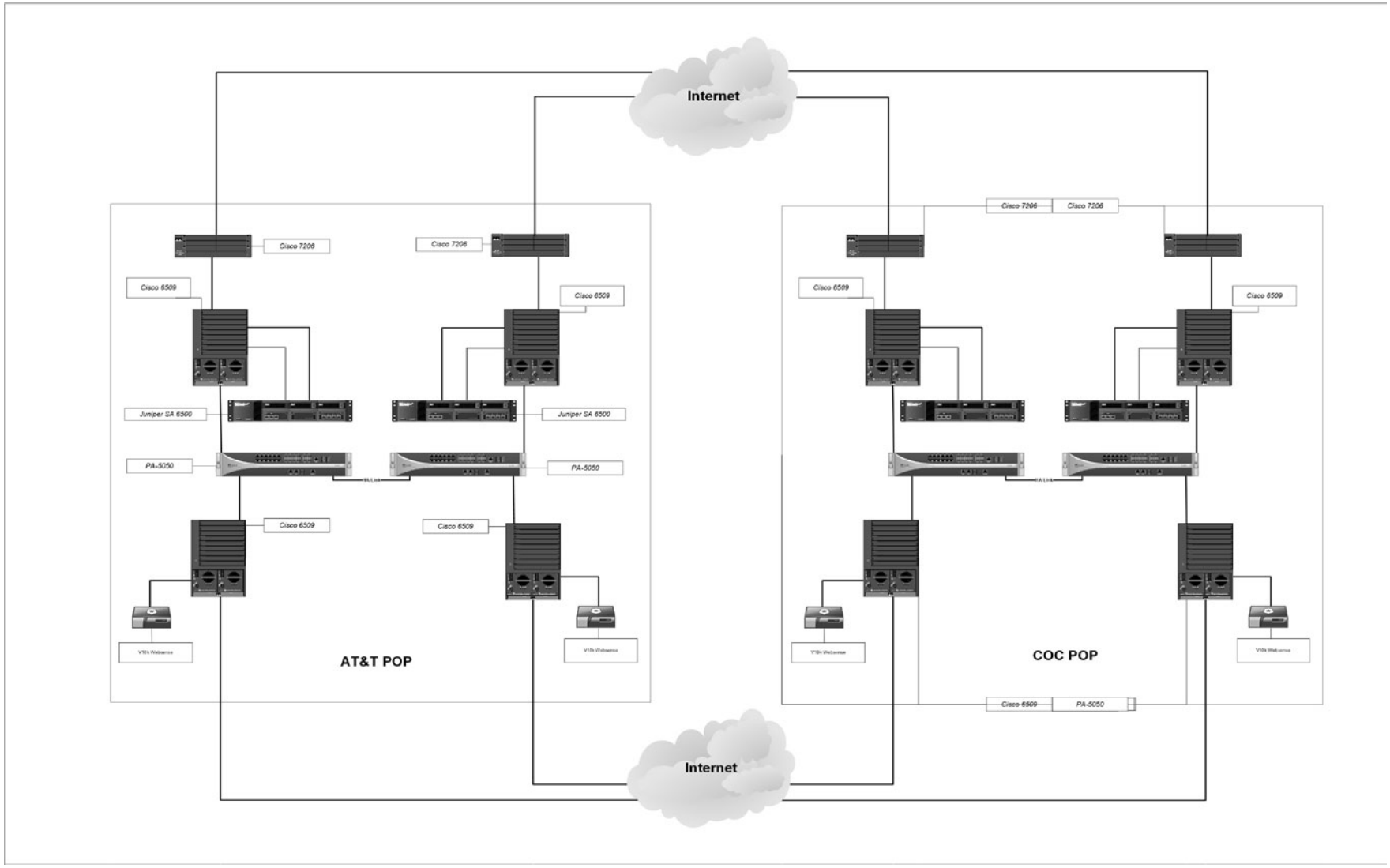
Using the PulseSecure client loaded on the County-managed laptops (as well as managed mobile devices once that project, which is currently in flight, is completed) allows full network access to any and all resources available to the user when connected on the County LAN. This client-based connection associates each session with a unique IP associated only with the specific user's SSLVPN connection for the duration of his or her connection. This connection is logged as well as tracked and reported as necessary, and it is used during troubleshooting activities that can be isolated to each user session.

At the user's discretion, a web portal connection is initiated by browsing to a URL and authenticating via the user's AD username and password. From within the browser session, users can perform up to three activities based on their membership privileges:

- **Initiate a terminal services session (remote desktop)** back to their own County desktop (if configured) or another County network device configured to accept terminal service connections. From there, users can perform normal LAN activity within that remote desktop session as well as create bookmarks for quicker access in future sessions.
- **Browse to County intranet sites** (such as Insite) using the browse function within the web portal window. Users can create bookmarks for these sites on their main web portal page.
- **Access file shares** that users have been granted permission to access, and create bookmarks to these shares.

All of these actions take place within the web portal window. Anything done outside of that window, including web browsing using a separate window or tab, does not flow to the County network.

Figure 64. County Geo-redundant Remote Access Services



Our Remote Access Services provide redundancy for constant uninterrupted access for County users

In addition to the host checking capability presently deployed, there are two remote access security features available for transformational use within the new Contract:

- **Security posture evaluation** assesses a device's security posture by determining the presence, versions, and levels of antivirus, spyware, and malware protection as well as operating system (OS) version and patch level, software patches, and disk encryption.
- **Role-assigned remediation** allows the restricted network access of devices for the sole purpose of performing remediation of any failed checks found during the security posture evaluation.
- This industry-leading solution is used by third-party vendors today to the direct benefit of the County. Our team manages 1,588 vendors who are assigned to 132 different group profiles so that each vendor group is allowed access to their resources only. In the future our team is fully prepared to load and configure the PulseSecure Connection software onto the computers of the third-party vendors so that they also gain immunity to a POP SPOF.

Another feature of our PulseSecure solution is direct support for smartphones and tablets provided by installing the PulseSecure mobile application onto these types of devices. However, due to inherent limitations with these mobile devices at present they cannot be configured to automatically sense the unavailability of one gateway and connect using the alternate.

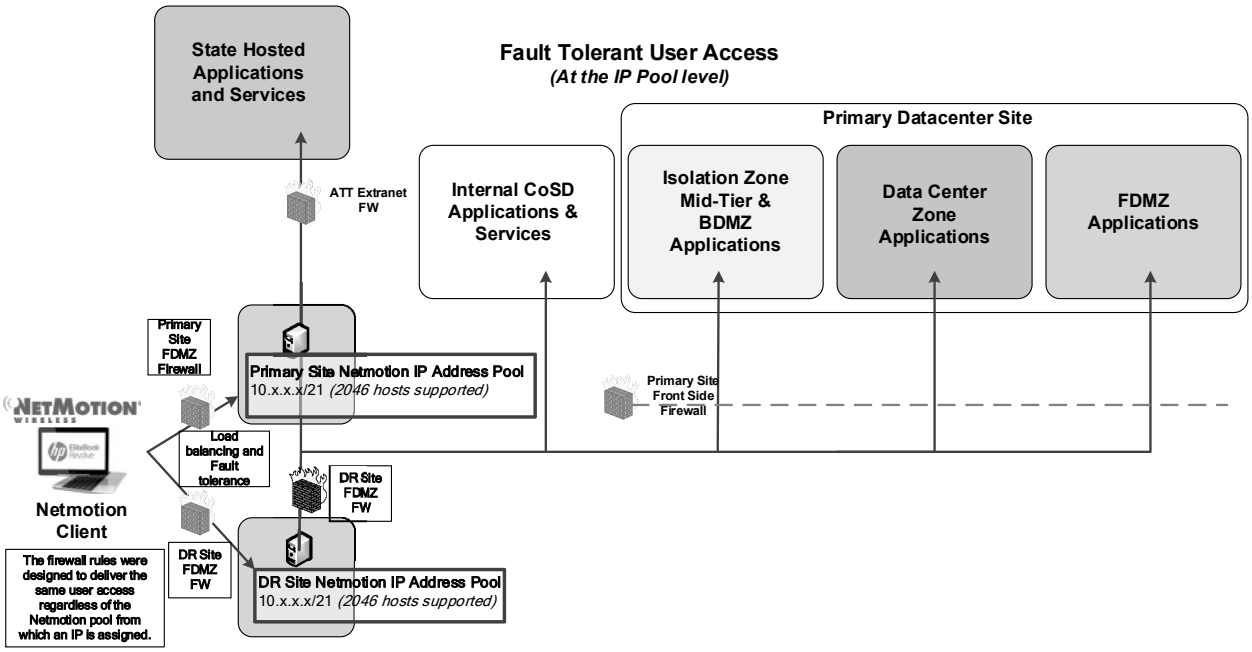
Currently the Pulse Secure mobile client is not "connection aware" and is unable to dynamically reconnect to a secondary gateway in the event the connection to the primary gateway fails. The Contractor has initiated feature requests and roadmap discussions with Pulse Secure to address the manual failover inherent to the mobile VPN solution for the County. If this feature does not become available in the first 6-9 months of the new term, the Contractor will evaluate and subsequently stand up a global load balancing solution such as F5's GTM(Global Traffic Manager). This solution would involve the installation of two virtual appliances leveraging our existing virtual infrastructure at both the POP and COC. This solution also possesses the potential to be leveraged for other services such as Mutare Voicemail to Email Service and could extend the capability of global load balancing to all solutions offered externally from the COC and POP.

NetMotion – Application Persistence (Virtual Private Network Level 2)

Our remote access solution includes application-persistent capabilities through our deployment of NetMotion Mobility VPN. Similar to the SSL VPN System, the application-persistent capabilities of NetMotion are enabled by assignment to the correct group profile, which also determines which specific application a user may access. Currently, there are approximately 1,200 mobile workers who require VPN connectivity and application persistence to support their business objectives and who require connectivity to the State of California as they roam between networks. In the new single data center model, NetMotion will be configured for high availability with redundant servers load balanced and will take advantage of the built-in redundancy within the data center for storage, network, electrical, etc., as well as the redundant connections to the data center.

The solution is to deliver an environment that supports mobility session persistence for County mobile workers as they roam wireless carrier networks throughout their business day. Also, it considers the internal County and external State network destinations to which mobility users must connect for successful business productivity. Connectivity to external and internal applications and services is a principal objective of our solution since the mobility infrastructure and applications will be behind data center firewalls. Another key objective is to manage the mobile user traffic efficiently so that business traffic traverses the links to the applications within the data center and internal County networks, but non-business traffic is redirected through the wireless carrier network or broadband connection. This capability is known as split-tunneling, and it will maintain the performance and security of the County's network. A depiction of the logical solution architecture is presented in Figure 65.

Figure 65. Fault Tolerant User Access



Transformation Opportunities

Potential future transformational activities are shown in Table 50.

Table 50. Potential Future Transformational Activities

FEATURE/TECHNOLOGY	COUNTY BENEFITS
PKI certificates on laptops	Expansion of current utilization for wireless authentication can be leveraged for remote access solutions as well.
Data loss prevention for data at rest	The ability to locate sensitive data stored in non-secured repositories.
Two-part authentication	Additional authentication and authorization of users and devices.
Consolidated application and network persistence services	Simplified support and user experience.

Similar to other activities that we have pursued in collaboration with the County, the features and benefits will be carefully evaluated within the Enterprise Architecture Forum with the CTO.

Our industry-leading remote access services meet the business needs of the County today and are poised to meet the County's future needs as well. Our experienced team members will continue operating as trusted technology advisors during these transformation roadmap reviews, emphasizing low-risk implementations and high return on investments as the "standard" for the new Contract.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

For continuity of our existing geo-redundant network and remote access capabilities, our solution uses the AT&T POP in the County as well as the County's Operations Center to hold the Mobile Access Gateways, VPN appliances, and to facilitate circuit terminations. The NetMotion application-persistence

solution is hosted on highly available and load-balanced virtual machines within the primary HPES data centers. HPES will maintain the NetMotion solution infrastructure in accordance with the standard procedures and policies, while supporting the application with guidance from NetMotion.

Working from our local facility, our SMEs will monitor, support, and maintain the remote access services. Any client side issue support will be initiated through our help desk process.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Through our routine involvement within the Enterprise Architecture Forum meetings, our SMEs maintain an in-depth understanding of the County's remote access needs and proactively prepare Solution Design Documents for County approval. Thereafter, our planning and testing of the proposed solution allows activations to go smoothly, with back-out plans executed if required.

When a new user or group of users requires remote access, we will gather requirements and determine the type of access needed. For SSL VPN and Application Persistence users, new users are placed into an Active Directory group with the appropriate level of access and security. For Mobile Access Gateway users, a Mobile Device Management (MDM) solution provides the appropriate level of access and security. We are continually evaluating new technologies and vendor roadmaps so that the most secure and reliable system with the highest performance is available to the County. Our past and current help desks have posted text-based information into Tier 0 repositories, and our team looks forward to working with the County to advance into video-based help desk files in order to better reach our customer support community.

Hardware associated with remote access will be refreshed on an ongoing 4-year cycle. This approach will be continually reviewed with the County, making certain that the refresh activities bring the greatest value to the County while offering continuous improvement to the service.

On a continual basis we will create, maintain, and update end-user training documentation and tips as well as associated help desk scripts pertaining to the remote access to match the version and features of the product.

To allow the maximum return on the County's investment, our proposed solution makes full use of the existing solution set, which can adapt to the County's future requirements. However, as the technology and requirements landscapes evolve during the new contract period, our SMEs will evaluate and propose new solution sets as needed to meet the County's needs and joint objectives.

- Automated Tools – Automated systems and tools involved in proposed solution

To monitor the remote access appliances and support the integrity of the remote access features, we use the CA Spectrum platform in conjunction with the Juniper JSA3800. The JSA3800 automatically collects logging information about all remote access connections and supports the routine review of the logs from a proactive as well as responsive nature. We have used these tools to respond to the County's ad hoc requests regarding specific user access activities, and we stand ready to support similar requests in the future.

- Qualifications and Experience – Background and experience in comparable environments

We will support the remote access solution using our local staff with extensive County network experience and an average of 9 years of experience with improving and transforming the County's network. Our network framework operations, project management, and engineering staff work directly with County departments and have learned County policies and processes, which help them design and implement the most efficient and cost-effective solutions. These staff members hold more than 34 distinct

technical certifications, including CISSP, CCNA, CCNP, CCDA, CWNA, and others. Our technical staff is required to complete targeted training each year to keep their skills current.

To support all components of the County network, our local technical team retains at its disposal a deep bench of subject matter experts, with the expertise and experience to handle any new transformative or operational objective or issue. While delivering our world-class support of the existing technology base, this pool of resources has the depth and breadth of knowledge that allows the team to analyze alternative technological/process options and support changing business needs.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

Over the life of this service PulseSecure SSL VPN has evolved to provide network persistence, at which time we observed an increase in adoption versus the NetMotion application-persistent service. Application persistence is more costly than standard VPN, with its use case being for mobile users who are interacting with enterprise applications while physically in motion. The Department of Animal Services is a perfect example of this case, where officers are operating applications on ruggedized tablets mounted in their vehicles. For these types of users application persistence is of great help, allowing their session to remain open regardless of connectivity. This example, however, does not apply to a vast majority of mobile users across the County. Most remote access subscribers are simply laptop users who rely on the connectivity they get through a VPN connection, while they operate from an alternate work location—not physically in motion.

As remote access technologies continue to evolve, HPES will seek to consolidate the network- and application-persistent capabilities that are currently being provided on two disparate platforms. This objective will take into account the current investment cycles and in turn the cost to the County, as well as the appropriate geo-redundancy of the design, performance of the solution, and synergies associated with a single support model.

At this time, our recommendation is to take a transformative approach to this goal, evaluating the best options for the County over the term of the Agreement.

Alternatively, the NetMotion service, provided out of the data centers, could be established as a standard for remote access services. This service provides application and network persistence and would do so under a single support model. Considerations to be made relate to disruption associated with migrating more than 2,500 laptop-, smartphone-, and tablet-based users to this new platform. Licensing costs would also need to be evaluated, which could have an effect on RU pricing and the flexibility for smartphone and tablet users to access MDM-based VPN as a right-to-use with a standard SSL VPN subscription.

Voice Services (Sched. 4.3, Section 5.7)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

As trusted advisors, our team fully embraces the County's strategy to use a process of continuous improvement to bring transformational change to County operations. This collaborative and trusted relationship begins with the evolving processes and governance. Working with the County, we have refined these working processes and methodologies during the present Contract and will continue to improve them during the life of the next Agreement. These activities enable us to identify, articulate, and deploy transformative solutions in the most cost-effective manner with minimal disruption to ongoing

business operations. This positive working relationship has resulted in numerous success stories and has built the foundation for future success. Our SMEs are constantly reviewing new and emerging technologies and determining creative and cost-effective ways to apply those technologies to benefit the County and its constituents.

Each transformational activity is initiated through the Enterprise Architecture Forum, where we provide ongoing architecture and management resources to facilitate the planning of upgrades, refresh, and strategic plans related to our voice services. In this forum, we perform the following:

- Maintain ongoing collaborative voice and unified communications roadmaps and architectural standards, with yearly reviews/revisions, enabling the continued advancement and adoption of emerging technologies.
- Identify single-point failures within the voice architecture and propose solutions for County consideration.
- Make recommendations to reduce County usage costs.

VoIP Services

In our current Agreement our SMEs recognized the need to build a robust, fault-tolerant data network infrastructure as a foundation for the convergence of technologies into a unified communications solution. The completed data network, which includes 802.1af PoE ports, now allows many aspects of the voice services to operate in a highly converged and highly redundant manner. In the new term, we will leverage this network infrastructure and build upon it by replacing older TDM and PBX technologies with Voice over Internet Protocol (VoIP) solutions that tie seamlessly into capabilities already implemented on the County network. As with other transformations, service changes must be completed within realistic cost constraints that provide demonstrable return on investment. Due to these real-world restrictions, our solution proposes significant reuse of existing assets that are current technology and well inside of the technology refresh cycle. We will reuse the major core voice-related appliances and associated licenses shown in Table 51.

Table 51. Major Core Voice-Related Appliances and Associated Licenses

AVAIL	IN USE	TYPE	DESCRIPTION
26,305	23,901	Aura Communication Manager-Core	Core license for CM stations
26,305	166	EC500	Extension to cellular
26,305*	277	One X Communicator	Softphone on desktop
26,305	0	One X Mobile	Softphone on mobile device
26,305	1	One X Communicator for Lync	Softphone on desktop for Lync integration
2,647*	2,647	Call Center Elite	Core call center software license
321	284	Elite Multichannel	Software for screen pops at ACCESS
484	452	Avaya Call Recording	Software for recording/ storage of agent/ customer voice calls
1,051	2,883	Call Management Agent	Per agent license for CMS
125*	309	Call Management Supervisor	Per supervisor license for CMS
12*	9	One X Agent	Desktop client phone for agents
175*	175	AAEP port	Experience Portal port license

AVAIL	IN USE	TYPE	DESCRIPTION
181*	181	AAEP CM Connection	Experience Portal to CM connection license
82*	82	Enhanced Call Classifier	Experience Portal call classifier license
117*	117	Nuance ASR	Experience Portal speech recognition license
117*	117	Nuance TTS	Experience Portal text to speech license
1,000	481	Mutare EVM	Mutare voice mail to email
1,000	481	Mutare giSTT	Mutare voice mail to text transcription
17,000	16,941	Modular Messaging	Voice mail licenses
26,305	200	Session Manager SIP connections	SIP licenses
3,758	200	Session Border Controller Trunk	SBC licenses for SIP connections
3,758	2	Session Border Controller Stations	SBC licenses for SIP connections

Part of any transformational activity is establishing a baseline through a clear and solid understanding of the current operational state. As the incumbent team providing support that exceeds the service level requirements (SLRs) our staff supports the existing voice services highlighted in Table 52.

Table 52. Existing Voice Services

VOICE COMMUNICATIONS PARAMETER	QUANTITY CURRENTLY SUPPORTED
Facilities supported by Centrex services	117
Facilities using TDM/PBX technology	81
Facilities using VoIP technologies	44
Single line Centrex handsets	295
Multi line Centrex handsets	127
Single line digital handsets	2,621
Multi line digital handsets	11,061
Single line VoIP handsets	1,050
Multi line VoIP handsets	5,229
Voice mail	16,000 out of 17,000 current licenses
Interactive Voice Response (IVR) services	111
Mutare (voice mail to email)	400 out of 1,000 current licenses
Auto Attendants	2,800
Automated Call Distribution (ACD)	200
Analog jacks	2,251
4-1-1 operator services	1

Within the new contractual Agreement, our staff members will apply their knowledge and skill sets to support continued operational excellence while deploying and maintaining VoIP and legacy services within the new quality of service parameters. Furthermore, our SMEs leverage this knowledge to continue transforming voice services with emphasis on equipment at or beyond life expectancy. As proponents of low-risk transformations, and in close coordination with the Enterprise Architecture Forum, our initial transformative services are projected to replace the TDM/PBX equipment at the 81 sites designated for transformation. This upgrade is proposed as an initial transformation initiative and included in Voice Services as a means to meet relevant scope requirements. Our complete Transformation Plan is described in Section 2.12, Transformation Services, subsection "Initiatives: Voice Services Transformation," as well as in "Initiatives: E911."

To support this objective our SMEs will work within the architecture forums and draft Solution Design Documents for the site transformations. Our formal solution design approval is then used by our project management team to develop implementation strategies and communicate with site-based County resources to upgrade each specified facility to VoIP services. These changes will reduce equipment footprint at each of the sites, while dramatically reducing the overall power consumption and increasing availability and reliability. Equally important, the upgrade will improve the user experience by reducing trouble tickets regarding set-based issues—such as speaker and cord problems—and will also provide new feature sets. For instance, the new VoIP handsets provide an integrated County-wide corporate directory for ease of searching for and contacting other County users.

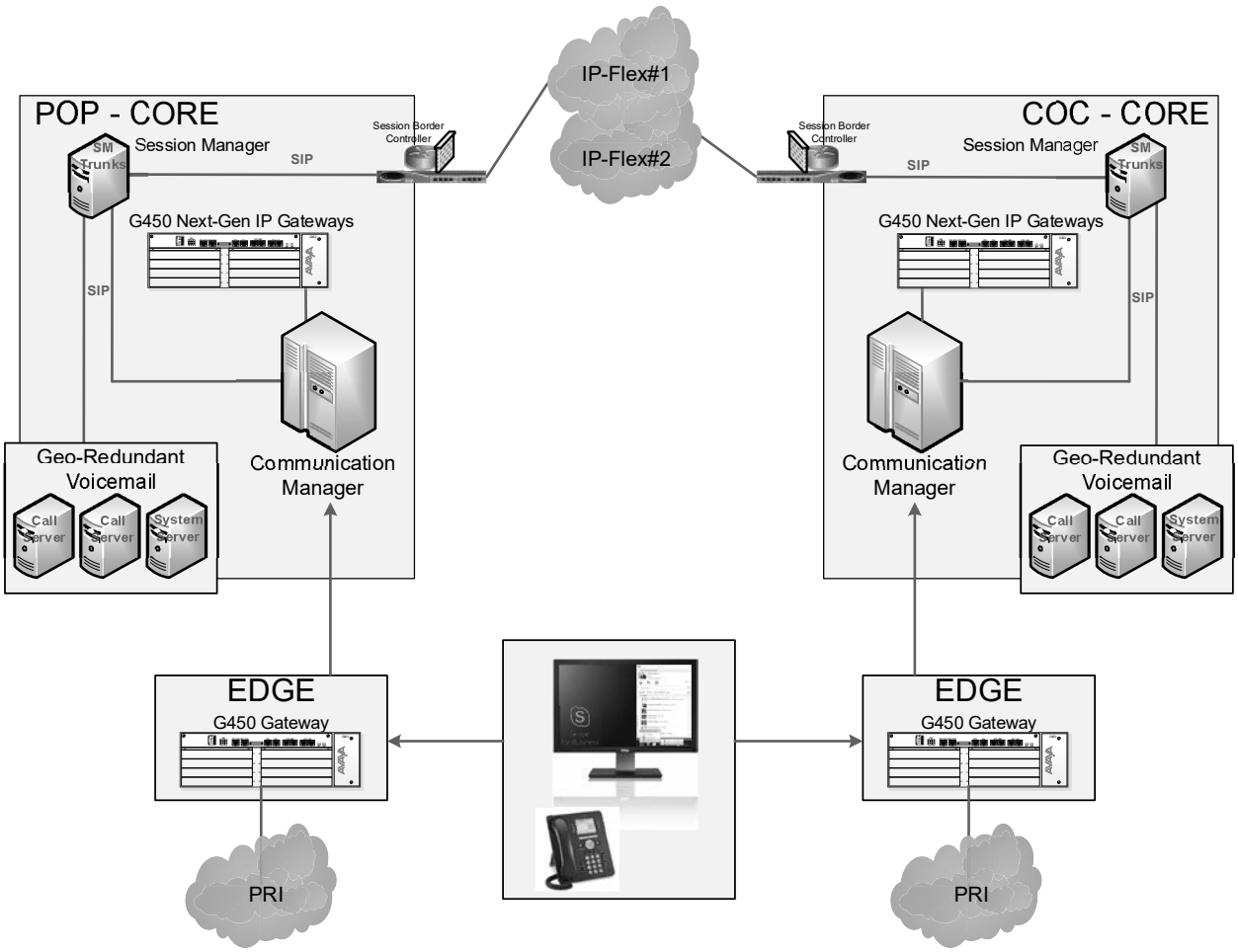
As a part of this upgrade to VoIP each site will also be migrated to a new E911 service, so that first responders have the necessary site and call location detail in the event of an emergency.

Leveraging the approach defined in the current Agreement, all new County sites will continue to be implemented with VoIP services as part of our ongoing efforts to continuously maintain technical currency and modernization of these services.

Geo-redundant Voice Mail

To enhance our current voice mail services, our solution plans to leverage a geo-redundant voice mail platform to provide a standardized voice mail experience across all County locations where enterprise voice services are offered. This solution, which is currently being planned for migration in 2016 to AVST with Neverfail, will include a phased migration of Centrex users to the new platform as these services are brought into new voice services standards. Figure 66 is a representation of the high-level topology of the voice mail solution that will be in place at the time of the Agreement if approved.

Figure 66. High-Level Topology



AVST with Neverfail provides geo-redundant, high-availability voice mail services.

Voicemail to Email Services

Another voicemail related feature is our continued support of Mutare speech-to-text service for transcribing voice mail messages into text with delivery to the user via email along with a .wav file to the County end-user email on a per-request basis by the County. This service is provided via a cloud-based platform.

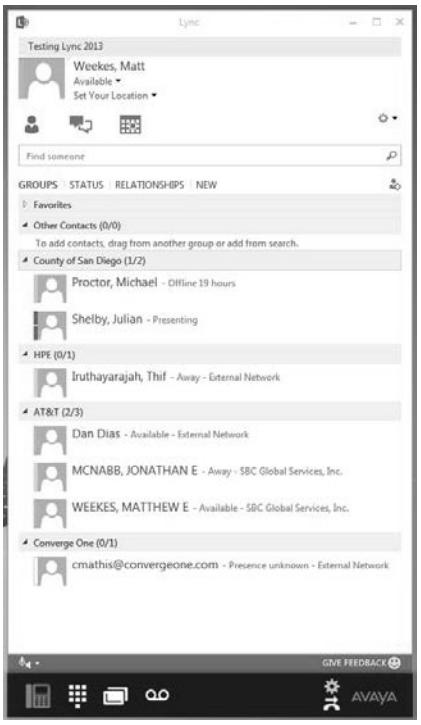
Unified Communications

Our team anticipates further voice service enhancements through the expansion of integrated desktop and handset functionality as part of our efforts to integrate voice services into unified communication services. For example, our SMEs recommend the deployment of Avaya Communications for Lync (Skype for Business [SfB]), Figure 67 and potentially the use of application plug-ins for Outlook because these software-oriented transformations provide direct user capabilities that increase the productivity of County business operations. These enhancements include complete call control from the Lync or Skype for Business client with the following key features:

- Click to call and click to answer from Lync or SfB
- Search and click to call from Outlook contacts

Outlook contacts match and screen "pop"click-to-conference

Figure 67. Lync Contact Screenshot



The Avaya Communications for Lync (SfB) embedded client enables integrated voice services through an application programming interface, providing a single client view.

Avaya Communicator Softphone

For users who require a more full feature telephony experience on their desktop than that provided by the Avaya/Skype for Business Client plug-ins, HPES will also continue to offer Avaya Communicator softphone functionality. This service allows remote and teleworkers a full featured software client, deployed upon request to their County provided desktop asset. Leveraging the connectivity provided by a direct LAN connection or Pulse Secure VPN/Netmotion, Avaya Communicator will allow users to make and receive calls from their designated county telephone number at their desk and remotely via a headset.

On-net Dialing and SIP Trunking

As noted previously, our solution to voice interconnectivity uses the robust, fault-tolerant solution deployed within the data network to provide resilient connectivity not only within the County domain, but as needed to support cloud-based solutions. This connectivity facilitates improved end-to-end collaboration and also reduces operational costs by implementing efficient local and long-distance dial plans. For instance, we have designed the local dial plan such that if a user tries to go off-net to make a call to another County location, that user is automatically rerouted back onto the internal network so that operational costs are minimized. Ongoing planning also includes capacity expansion of the existing SIP trunking internally and externally for increased efficiencies. As an immediate objective, our team will expand the capacity of existing SIP services, configuring them to support not just local calls but also long-distance and toll-free (800) calls. This will eliminate usage charges for all outbound domestic calls from the enterprise and substantially reduce the usage charges for toll-free 800 inbound calls.

Centrex Migration

Although the majority of voice services are provided by the Avaya enterprise voice network, a small subset of County of San Diego sites have their voice services delivered by AT&T's Centrex business telephone service. The Centrex service is deployed to smaller County of San Diego sites with as little as 1 user up to 20 users. At present there are more than 117 sites with Centrex voice services many of which are in remote locations. Although Centrex services provide stable telephony and voice mail services, these locations are disparate from the rest of the County user population and are not able to take advantage of the full Unified Communications (UC) capabilities offered to Avaya enterprise users. Migration of these Centrex voice services locations to the Avaya architecture is becoming an increased business priority. AT&T has developed a transformation approach to migrate a majority of these users/stations to a VoIP solution, while maintaining a roadmap for remote and intentionally off-net services to be executed over the term of the Agreement. This effort is planned for implementation early in the term as a transformation

initiative and is included in the proposed Voice Services. Further details on the migration of Centrex users are in Section 2.12.

Basic/Simple IVS Solutions

Our proposal includes the support of Auto Attendant and Automated Call Distributor services as a right to use feature for subscribers of Voice Services. This basic functionality is inherent to the Avaya enterprise telephony network. This proposal will enable 39 previously billed "Simple" IVS resource units to consume the service no additional charge.

411 Operator Services

In 2015, AT&T upgraded the IVR that supports the County 411 information line, providing additional self-help capabilities and bilingual voice recognition. This new service has provided improved efficiency in delivering County and public users with County information. These services will continue to be supported in the new term, including a live operator option for users and constituents who "zero" out of the IVR. Over the life of the Agreement, additional recommendations will be developed and proposed to enhance and improve this important service.

800 Toll-Free Services

Toll-free services for publicly dialed County telephone numbers will be supported by AT&T and provided at a significant price reduction relative to current rates.

In fulfilling roles as trusted partners, we have focused on incremental and iterative feature advancements to the voice services, increasing the "stickiness" of the solution and enabling increased end-user productivity. As we reach this tipping point in the integration of voice and unified communication services we are reminded that the sometimes long road to transformation ultimately relies on disciplined planning and the ability to recognize and seize opportunities when they become ready for the enterprise.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Our team provides dedicated, local voice resources on a 24x7x365 basis for the County today, and we will use this same approach during the new Agreement. Our staff members are highly trained and knowledgeable workers who have supported every business unit within the County and understand its unique operational and procedural needs. This approach significantly reduces the operational risk of deploying new staff resources and the associated learning curve to obtain any level of customer familiarity.

In support of voice network services, the local technical team retains at its disposal a deep bench of subject matter experts who have the expertise and experience to handle any new transformative or operational objective or issue. This pool of resources has depth and breadth of knowledge that allows the team to analyze alternative technological/process options and provide recommendations for change.

Because the voice services component leverages and follows our data network services deployments, the associated voice service appliances will reside within the same facilities used by the network for resilient and fault-tolerant services for the service level requirements. Over the course of the new Contract these facilities will also be leveraged as entry/egress points to cloud-based voice services.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

To better support our user community, our team has placed documentation onto our Tier 0 Service Portal that provides "how to's" for key aspects of new voice services that we provide. As an integral part of any

deployment, we review this documentation for currency. During the new Performance Contract we anticipate formally requesting County approval to develop and deploy short videos for the Tier 0 Service Portal to better serve users who would prefer to see how to do something rather than read a document.

For end-user support within the new contractual service level requirements, our team will continue our multi-tiered service and support structure. This structure provides the appropriate skills at each level to handle incidents, coupled with a clearly defined escalation management process to facilitate proper incident response and resolution. In addition, we use a complete set of automated tools, which drives quicker response and resolution and minimizes impact.

Each platform/service type uses a predefined set of operational processes that have been refined throughout the present Contract period so that we achieve customer satisfaction and service levels. Our team leverages the Nectar Unified Communication Management Platform to access knowledge modules to assist with identifying and resolving issues. Also, we leverage a SharePoint Services Knowledge Base that provides a customized set of knowledge and process tools specifically reshaped over time for use by the County's voice service response team. Our team has developed a voice-specific internal SharePoint Wiki that has complete infrastructure documentation organized by site.

- Automated Tools – Automated systems and tools involved in proposed solution

For quality voice service within the service level requirements defined by the new Agreement, our SMEs use numerous automated tools. These tools enable us to continuously monitor the overall health and performance of voice appliances, assist in rapid restoration through fault isolation, and perform traffic analysis—discussed further as follows.

Our team delivers complete manufacturer system maintenance coverage on all County core voice services assets. The Avaya maintenance services include Avaya Expert Systems and Secure Access Link. Avaya Expert Systems provides the County core voice services with a maintenance database of more than 30,000 Artificial Intelligence Algorithms (AIAs) with scripted automation that is able to correct many known system- and software-related issues automatically. Avaya Secure Access Link (SAL) is a centralized consolidation point for all Avaya Core Systems for health and alarming monitoring, secure remote access using secure outbound-only HTTPS standards, and an integration point for Avaya Expert Systems. Together these tools provide the County's Avaya core voice services with complete health monitoring and expeditious issue resolution. Avaya Expert Systems and Secure Access Link are online and engaged 24x7 to diagnose and attempt to resolve known system alarms, clear many service-affecting issues, and escalate issues to engineering resources for prompt attention when necessary.

Our voice services team uses Nectar's Unified Communication Management Platform (UCMP) and its complete suite of innovative features to provide the County with enhanced, integrated Unified Communication network services. Nectar provides multi-vendor management services, including application dependency tree visual alerting and vendor knowledge modules, which help our SMEs proactively pinpoint and resolve cross-platform integration issues quickly and restore services to County users. The UCMP includes real-time network quality of service reporting using RTCP integration and can create simulated traffic injection between designated network segments for analysis. This allows the SMEs to monitor and report on all VoIP-related traffic transmissions. The quality of the service reporting tool provides per-hop statistics and in many cases assists in quickly identifying improper packet handling hop points—driving efficient resolution of network quality of service issues. The Nectar UCMP includes statistical resource utilization data gathering and storage that enable trending analysis and capacity planning so that County users are not impacted by growing resource needs. Finally, all of these capabilities are available using an intuitive and customizable dashboard with visual and electronic alerting from sophisticated threshold configurations. The dashboard allows us to acknowledge, respond, and correct issues proactively—in many cases before County users know or report an issue.

- Qualifications and Experience – Background and experience in comparable environments

Our team's support specialists participate regularly in internal and manufacturer-led training programs. We hold certifications specifically related to Unified Communications Systems and have been recognized by technology leaders for our support expertise. Our certifications include the following:

- Avaya Certified Expert – IP Telephony
- Avaya Certified Implementation Specialist – Unified Communications
- Avaya Certified Implementation Specialist – Contact Center
- Avaya Certified Solution Specialist
- Cisco Certified Network Associate – CCNA
- Cisco Certified Network Professional – CCNP
- Microsoft Certified Solutions Expert – Lync Master.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

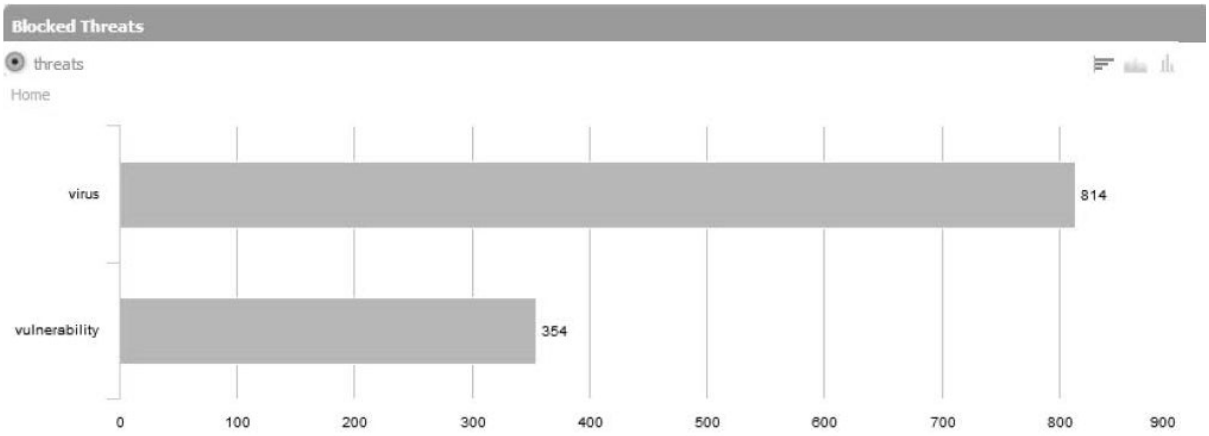
Network Security Services (Sched. 4.3, Section 5.8)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Late in the current Agreement our SME's collaborated with the County to design and migrate to a new robust security infrastructure using the latest in next-generation firewalls, unified threat management, and data loss prevention (DLP) technologies. This decision was made after taking into account an emerging shift in the industry, which was significantly disrupting vendor strategy across the network security landscape. This transformation was one of the most substantial efforts from both a complexity and potential impact perspective the network team had ever undertaken over the life of the existing term. We are proud to report that the implementation of these advancements was completed not only without incident, but more than 3 months ahead of schedule. This current, progressive security infrastructure solution will be leveraged as HPES seeks to further improve the security posture of the County network. The following components are included in our services proposal:

- **Palo Alto next-generation firewalls with unified threat management capabilities.** These appliances provide not only firewall services, but they also provide intrusion detection/prevention (IDP), spyware and AV filtering, and web content filtering. Automated, daily threat updates allow the County network to be protected against the very latest in malicious content and activities. Extensive reporting capabilities in this solution (as shown in Figure 68 and Figure 69) enable deep dive views of network communications to highlight the possible effects on network performance. This solution also provides automated alerting of possible malicious activity for immediate investigation and remediation.
- **Websense cloud-based content filtering.** This technology further protects County assets, even when outside the County domain. By replicating content-filtering policies in use on the local County network to the cloud-based service, we are able to support continuity of protection across all avenues of connectivity in use by County personnel, regardless of their physical locale.
- **Websense Data Loss Prevention (DLP) for web channel and data in motion.** This service prevents sensitive data (personally identifiable information [PII] for instance) from being transmitted outside of the County network in unencrypted communications or copied to a removable device (i.e., thumb drive).
- **Advanced Distributed Denial of Service (DDoS) detection and protection.** This service protects County Internet circuits and provides security event analysis and correlation via live 24x7x365 monitoring.
- **Tenable Security Center.** Continuous perimeter scanning provides a close to real-time view of supported and non-supported inventory, including real-time threat updates and monitoring of vulnerabilities and risk, as well as close to real-time asset status updates. This provides an improvement to the snapshot in time information that is currently available.

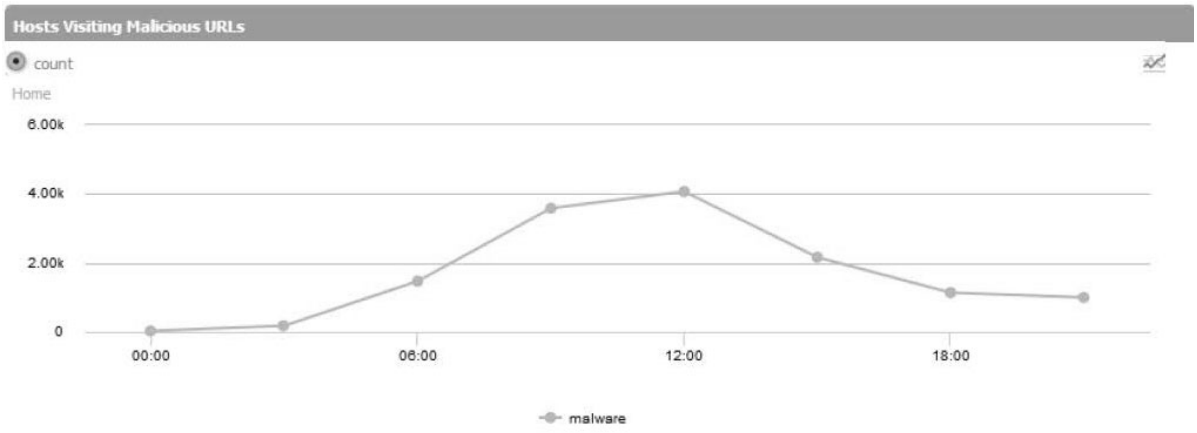
Figure 68. Security Reporting



Threat Name	ID	Threat Type	Threat Category	Severity	Count
Virus/Win32.WGeneric.hnher	2445166	virus	unknown	medium	725
Microsoft Windows Shell .lnk File Remote Code Execution Vulnerability	33351	vulnerability	code-execution	critical	316
Virus/Win32.agent.kig	2022855	virus	unknown	medium	89
Microsoft Windows Print Spooler Service Impersonation Vulnerability	33427	vulnerability	code-execution	critical	21
ANGLER Exploit Kit Detection	37744	vulnerability	exploit-kit	critical	10
Microsoft Windows Print Spooler Service Impersonation Vulnerability	34163	vulnerability	code-execution	critical	6
Microsoft IE GIF Parsing Double Free Vulnerability	30025	vulnerability	code-execution	critical	1

Security reporting from the Palo Alto next-generation firewall shows the threat-blocking capability of the existing infrastructure.

Figure 69. URL Filtering



Source Address	Source User	Count
10.35.181.195	None	7.3k
10.144.108.103	None	4.1k
10.37.147.127	None	360
10.50.66.100	None	184
10.61.65.155	None	154
10.50.48.183	None	138
10.35.177.128	None	124
10.38.241.118	None	119
10.50.19.188	None	115
10.145.5.148	None	105
others	others	997

Security reporting from the Palo Alto next-generation firewall shows malicious URL filtering.

Transformation Opportunities

As part of our team's dedication to continuous improvement for the County, efforts are currently underway to increase functionality in many ways:

- **Application-level security policies.** By moving from port/protocol-based firewall policies to application-based policies the tools can fully inspect traffic flows. This type of technology safeguards against programs attempting to use non-standard ports to circumvent port/protocol-based security. Our team may refine security policy to data flows, as well as determine the types of applications in use on the County network. This enables us to provide more in-depth assessments and recommendations for network enhancements.
- **User identification.** By providing positive identification for each user tied to a data transmission, firewall policies can be written to allow authorized network communications based on user ID rather than an IP address. Consequently, the policy is in effect for the user, regardless of his or her location on, or entry point into, the County network. This solution eliminates the need for static IP addresses for firewall policy mapping—thereby providing better policy management without the need to map policies to entire subnets to accommodate the mobile nature of today's workforce.
- **Active Directory group-based policies.** Much like user identification, AD-based policies allow for the mapping of security policies to specific groups created within AD. This allows for a security policy to be applied to all users who are members of an AD group, regardless of where they reside on the County network. For example, if a member is added to the HR group then he or she automatically inherits the security policies applied to that group without having to have a firewall change made to accommodate him or her specifically. As a result our SMEs have greater flexibility in mapping security to user roles without increasing complexity in either process or implementation.
- **Network Access Control (NAC).** NAC for both the wired and wireless environments is presently being scoped for deployment. This capability provides appropriate levels of network access based on the device being connected. County-managed devices are given full access to the County network just as they are today. Non-County devices are segregated on the County network and allowed only access to the Internet unless otherwise authorized through a formal review process. More detail on our Network Access Control solution can be found in Volume 2.08.1, Section 2.8.9.
- **Integration with the County's PKI solution.** This effort is in progress for device authentication for wireless devices, as well as device and user authentication for mobile VPN connectivity. These integrated solutions guarantee that only County-authorized devices are able to connect using County wireless networks or via the County's SSL VPN solution. This approach effectively isolates the network from exposure to non-County managed devices that could pose a security risk.
- **Websense Data Loss Prevention (DLP).** This solution for County data at rest is now in the early project stages. The DLP solution is already in place for data in motion and web channel, protecting against the release of sensitive data onto the public network or transfer of data to removable devices. The next phase of that will enable the scanning of repositories to identify sensitive data being stored in non-secure locations.

In each of these cases the solution currently provided or being proposed is based on the best industry products with a view toward improved security and increased performance. Each of these solutions has been carefully evaluated against other potential solutions and found to provide superior capabilities to deliver improved security to the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The existing local LCM team consists of network security personnel who are dedicated to the County program to support all aspects of the network security framework on a 24x7x365 basis. All security components have been designed for redundancy and resiliency to preclude single points of failure.

All hardware and software used to provide network services from the AT&T POP location are contained in a secure location, accessible only by AT&T personnel or those they escort. All personnel having access to County associated devices at the AT&T POP have undergone background checks and verification. Security measures include guarded access, with signature and ID required for admittance along with biometric security.

Access to network services hardware and software located at County facilities will be managed by the County.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

All software versions will be evaluated upon release with consideration for feature benefit and risk, with intent to maintain an "n" standard. Any deviation from standard will be mutually agreed by both HPES and the County. Patches and updates are evaluated as they are made available to determine their applicability to the County environment and will be deployed immediately as needed.

The continuous 4-year refresh cycle is applied to security hardware as it is to all network refresh activities. The hardware and systems are continuously evaluated so that they can meet the requirements of the County's high-speed network and are upgraded as needed.

We perform the configuration of the hardware and software using industry best practices—resulting in hardened, or locked down, systems. We remove default usernames and passwords, disable unnecessary services, and all management communications to and from the devices are via encrypted connections.

An ongoing evaluation of current and emerging technologies has allowed our team to continue providing the County with the highest level of security by using the latest in security technologies while building for the future. By developing a perpetual security-centric roadmap in cooperation with the County, our team has closely aligned the recommendations and implementations of security technologies with the County's priorities and vision for network services.

- Automated Tools – Automated systems and tools involved in proposed solution

A centralized management platform delivers strict change control along with powerful reporting and alerting capabilities and automated notification of security events. The threat profiles currently in place are identifying tens of thousands of possible threats across all categories (IPS, AV, Malware, and URL) each day.

These threats are captured by AT&T's local San Diego vendor, Security on Demand. They perform analysis against the data, including behavioral analytics, to determine whether there is a potential threat. If such a threat exists, or further analysis with the LCM team is required, then a ticket is generated or a call is placed directly to our dedicated security staff for high severity issues.

The logging mentioned above as well as all of the logging from the HPES security devices is fed into the security information and event management (SIEM) solution for analysis and triangulation against other security data sources such as data center firewalls and intrusion prevention systems/intrusion detection systems (IPS/IDS).

Automated email alerts are also delivered daily to the dedicated HPES security staff by our Palo Alto environment, where additional analysis is conducted and fed to the Cross Framework security team and Cross Framework capacity and performance team. Finally, our Security team uses these tools to develop recommendations for evaluation by the CISO and CTO Security lead.

From this analysis, possible actions may be generated to include but not limited to scanning of devices, removal from the network and reimaging of desktop devices if necessary (for County assets), and

configuration of network or URL blocking and tuning of threat signatures. Investigations are conducted to determine whether hosts have fallen victim to malicious activities and what the impact or spread of those may be. All investigative reports are provided to the County for their review.

In addition, monthly reporting is provided to the CISO for review with PMO Security on both threat alerts and URL blocking taking place in the County environment. This allows both trending analysis and the development of future security strategy roadmaps. Figure 70 and Figure 71 are sample counts of blocked URL categories shown on the County network for a 30-day period.

Figure 70. Report Showing Counts for Blocked URL Categories on County Network

Category	Count
malware	512.21 k
Staff Global Blacklist	4.46 k
phishing	2.21 k

Sample Report: This example shows actual counts for blocked URL categories identified on the County network during a 30-day period.

Figure 71. Report Showing Threat Types on County Network

Threat Types

Top 5 Spyware

Spyware	Count
Suspicious DNS Query (generic:0171.upd..	18
Suspicious DNS Query (generic:hzgepqss...	9
Suspicious DNS Query (generic:intspoken..	8
Suspicious user-agent strings	6
Suspicious.Gen Command And Control Tr..	4

Top 5 Vulnerabilities

Vulnerability	Count
IBM Lotus Domino nLDAP.exe Remote ..	259,771
HTTP Unauthorized Brute-force Attack	11,228
DNS ANY Queries Brute-force DOS Att...	9,504
HTTP: User Authentication Brute-force ...	7,624
Microsoft Windows Print Spooler Buffer ..	4,856

Top 5 Viruses

Virus	Count
Virus/Win32.WGeneric.hnher	725
Virus/Win32.agent.kig	89
Trojan/AndroidOS.guerrilla.e	4
Virus/Win32.WGeneric.eeybx	3
Virus/Win32.WGeneric.hoqth	3

Sample Report: This example using extracted County data shows the Top 5 threats identified across multiple categories for a 24-hour period.

This in-depth automated logging, correlation, and alerting provide greater levels of security to the network and protect County assets, resources, and business data.

- Qualifications and Experience – Background and experience in comparable environments

The dedicated LCM team consists of members who hold strict, high-level, industry-recognized certifications in multiple aspects of IT security, including Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification Certified Intrusion Analyst (GIAC GCIA), Global Information Assurance Certification Auditing Wireless Networks (GIAC GAWN), and Palo Alto's Accredited Configuration Engineer (ACE) certification.

The group's technical skills and experience, coupled with a deep understanding of the County's business needs and goals, enable our team to implement substantial transformative initiatives in a highly compressed timeline with minimal impact to County connections.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Video Conferencing Services (Sched. 4.3, Section 5.9)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The County has primarily used traditional room system and roll-about personal video teleconferencing systems for mostly internal applications within the County domain. Use cases currently using this traditional conferencing capability include court video arraignment and remote tele-psychiatry services, as well as regional business unit offices.

The existing County telepresence services allow end-point video units to use the centrally located Tandberg Management System (TMS) and Cisco Video Conferencing System (VCS) platforms for gateway and scheduling services. The core TMS and VCS platforms enable closed circuit and point-to-point video conferencing services across the internal IP network using H.323 protocol. The TMS contains an electronic phone book of related business units within the County along with other business units in the County. The TMS is used to manage the VCS equipment that actually establishes the conference calls.

With the expansion of desktop and mobile client-based video functionality, there is increased business value in enabling cross-platform video conferencing systems. With such a system, video can become a more pervasive means of meeting with County employees and constituents. To meet these emerging needs our team proposes the continued use of existing video conferencing capability in conjunction with a cloud-based solution to fulfill all of the County video conferencing requirements. However, to remain compliant with required equipment refresh cycles, part of our solution replaces the TMS and VCS with the Cisco Unified Communications Manager (CUCM) virtualized appliances, which will be implemented in a geo-redundant configuration between the AT&T POP and the County Operations Center.

As mentioned, there is an increased need to provide an integrated solution that enables room systems and roll-about personal video teleconferencing systems to interact with desktop-based video capabilities. These solutions will enable onboard or peripheral camera devices to join multi-point conferences using either a web interface, Microsoft Lync (Skype for Business), the Unified Communications client, or via a mobile device. As a part of our collaborative roadmap and planning effort, our SMEs evaluated several different alternatives. Due to the ongoing County investment in Office 365, this has included a potential Microsoft solution. However, this option does not presently allow the cloud-hosted Office 365 tenant to

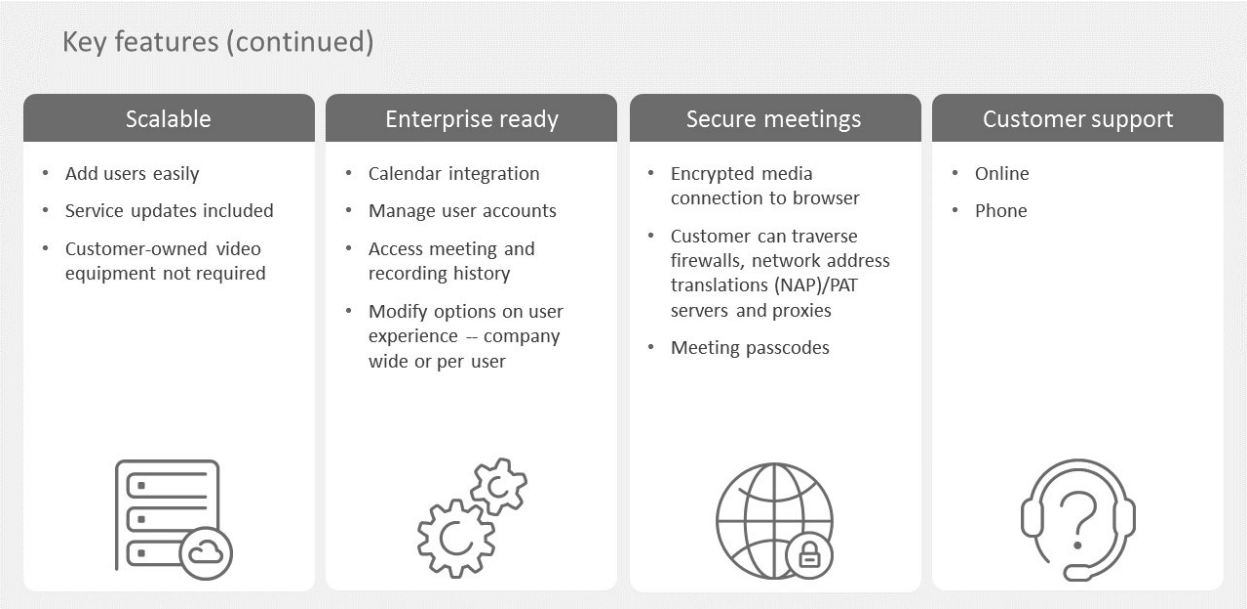
integrate directly with on premise infrastructure solutions without significant investment on behalf of the County. This type of analysis demonstrates our local team's foresight and alignment with the County, where we act on behalf of the customer to evaluate and determine the most appropriate solution to meet the needs of the business.

To fulfill the need for a fully integrated video teleconferencing solution our team is proposing AT&T Meetings with BlueJeans. This solution offers a cloud-based video bridging capability that can integrate services like Skype for Business and Google Chat with traditional standards-based room video systems. The system is scalable, device and platform agnostic, and provides a flexible yet standard platform for video teleconferencing. Features of this integrated solution is depicted in Figure 72 and Figure 73.

Figure 72. BlueJeans via AT&T

The hosted Meetings with BlueJeans via AT&T provides full interoperability across many platforms and allows for many types of collaborative, real-time interaction.

Figure 73. Hosted Meetings with BlueJeans via AT&T



The hosted Meetings with BlueJeans via AT&T scales easily both internally and externally, while providing additional enterprise and security capabilities.

As the County continues to evaluate and implement services, such as NetBond, AT&T can redirect the videoconferencing traffic from ISP connections to a private MPLS connection—providing additional performance, scalability, and security.

This Meetings with BlueJeans solution leverages the availability of existing videoconferencing units around the County and facilitates interoperability with the existing Skype for Business clients for extended telepresence. Users can participate from anywhere using any device—with a dedicated app, a web browser, or the Skype for Business mobile application.

From a desktop/laptop/tablet/smart phone user's perspective, the Meetings with BlueJeans experience is as easy as clicking on a link in an email or a meeting request. The Outlook plugin adds the capability to schedule meetings using a personal meeting ID or a dynamic meeting ID. Users can also edit default meeting preferences and add/edit/cancel meetings. The additional support for delegate scheduling allows executive support personnel to schedule meetings on behalf of executive staff. From an existing Cisco videoconferencing unit, a user simply dials by inputting the IP address as listed in the invitation.

Additionally, the Meetings with BlueJeans hosted solution allows numerous customizations, including the ability to set language preference, meeting passwords, entry tones, meeting security controls, and more via the web-based user interface. Features such as the high-definition content support, video sharing, and the ability to record meetings coupled with the integrated encryption allow the County to conduct video meetings securely as desired today and into the future.

As an example of the HPES team's ongoing commitment to continuous improvements, AT&T has completed a proof of concept in 2015 that validated all functionality between the existing on premise, Cisco-based solution and BlueJeans connected devices. This successful test brought together, on a single conference call, a County desktop with Lync, a County Cisco room system, a smartphone with a BlueJeans client, a wireless connected laptop using Lync, and a wireless-based laptop using a browser on a single conference call. Leveraging this type of functionality new business cases will undoubtedly be found by County departments. One such case could include a Registrar of Voters Election Day kickoff to

its regional polling stations, where the Registrar could kick off an election day live via video to his or her volunteers.

Based on the completed proof of concept and related engineering analysis by our SMEs, our proposed solution can be activated expediently with minimal risk to deliver the needed functionality of expanded video conferencing across all platforms.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Our solution uses the existing video conferencing solution set and the associated facilities that house the equipment today, including core infrastructure in the AT&T POP and the County Operations Center. Furthermore, our existing local staff will continue to support the video conferencing services as well as all of the other framework components from our County location. This local staff is also responsible for continuous development, maintenance, and updates of all items associated with video conferencing, including help desk scripts, training documentation, and processes for end-user support—and this staff continually provides new and updated material to support operational needs.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

As part of our ongoing commitment to continual improvement our SMEs will continue to evaluate solutions and introduce them through the weekly network architecture meetings and thereafter through the Enterprise Architecture Forum. These iterative processes allow our proposed solutions to address known and projected business requirements, convey direction, gain insight regarding other project path implementations, and allow required approvals as well as maintain consensus.

Our team uses insight gained from the ongoing operation and maintenance of the infrastructure to assess potential transformational, refresh, and upgrade activities. For example, our analysis has suggested a replacement of the TMS and VCS with the virtualized CUCM implemented in a geo-redundant configuration to eliminate a single point of failure. If other SPOFs are identified and remediated then our SMEs understand the processes and documentation to effect the change with minimal effort by all parties involved. Our local, dedicated team provides the coordination of resources necessary to plan, design, and implement the video and archiving solution. All work efforts and problem reports flow through the existing processes in place for support of the County's network.

When a business unit at the County requires video conferencing they submit a request via an Install/Move/Add/Remove (IMAR). Our team receives the IMAR request, gathers information, and designs a solution that we present for approval. Once approved, we order, receive, and stage the equipment and other necessary components for installation. We coordinate the installation date with the end user or business unit, and we dispatch a technician to complete the installation.

Based on the projected demand and the anticipated evolution of video conferencing services, we engineered a solution that provides services to meet the County's requirements without excessive costs for licenses that may not be used or will be eliminated/replaced overtime. The BlueJeans integrated video teleconferencing offer included in our proposal includes a 100-host license, where designated video conferencing hosts will be identified by the County. These 100 licenses represent simultaneous conferences, as only one licensee is required per conference. These licenses are dynamic and can be changed in real time to different users via the scheduling portal. There is one consideration that the County should evaluate: With the wider adoption of standards-based systems like Skype for Business/O365 and the anticipated product enhancements of O365, there could actually be less of a demand for the BlueJeans-based services over time.

Over the life of the term, the wider adoption of standards-based systems like Skype for Business/O365 along with anticipated industry enhancements could shift the solution for multi-platform video teleconferencing. The Contractor believes that the Microsoft's planned development of multi-platform transcoding via a Skype for Business mediation server could position the County to move towards a Skype based standard for all video teleconferencing services. The Contractor will work with the County to evaluate such options and make recommendations accordingly.

- Automated Tools – Automated systems and tools involved in proposed solution

In addition to the TMS and VCS platforms as well as the CUCM we have just discussed, our engineers and help desk staff also use CA Spectrum and eHealth to monitor the operational status of the appliances and the bandwidth usage so that we meet the service level requirements. The BlueJeans solution offers portal access to evaluate user and conference usage and detail.

- Qualifications and Experience – Background and experience in comparable environments

Our team has years of experience providing existing Cisco-based video teleconferencing services to the County. As our reach into the unified communications space evolves and desktop and mobile clients become a primary platform for video conferencing capabilities, our team is expanding its depth and breadth of skill sets to meet the need. From our own pool of SME resources to vendor support personnel, we have a deep bench of leveraged resources to draw upon as strategic and operational needs arise.

AT&T's partnership with BlueJeans also provides enhanced support to assist in the remediation of any interoperability issues encountered. These combined service capabilities allow us to meet the service level requirements.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

The HPES network team also proposes an alternative approach to video teleconferencing services that would sunset the existing Cisco/Tandberg platform and services, with a migration approach that would standardize on a Skype for Business (SfB)-based solution. With this approach, existing Cisco end points would remain in service, but they would be limited in their support as new SfB personal video systems were made available via OIC. For the large room systems a standard model would be identified, which could be obtained via the resource unit.

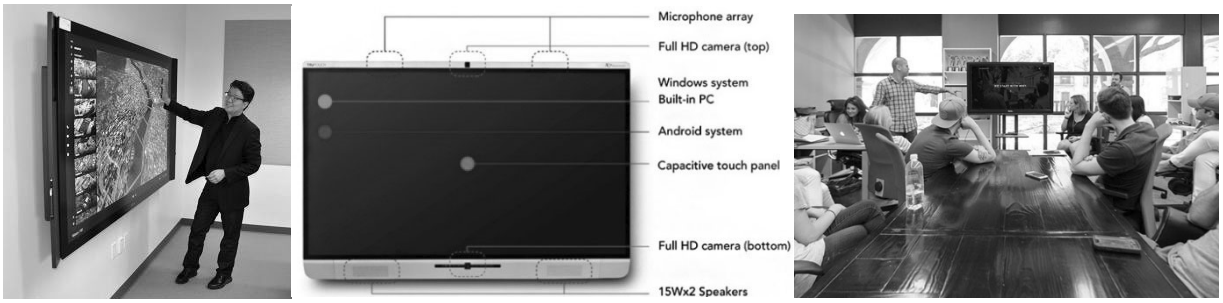
By moving to a Skype for Business standard, all devices and users with access to SfB would be supported, including laptops, desktops, and mobility devices using the SfB client or mobile application. This enables participation and interaction from anywhere, removing the current requirement to have physical access to VTC hardware to participate in video conferencing. This capability could lead to increased use of video, including multi-point conferencing.

This capability is currently available to the County via its existing Microsoft Enterprise Licensing Agreement (G3) and is used today in some limited cases to conduct video meetings outside of the managed VTC offering. This inherent capability within the currently licensed product set will allow meetings within the County user base as well as outside partner agencies via web browsers or Skype for Business client software installations on a variety of platforms, including many existing Skype for Business-compliant room systems inside the County. This approach will remove the device barrier and

allow for all managed devices to participate in video conferencing, providing they are running the SfB client or mobile app. This common-sense approach will allow for a single video conferencing platform standard across the County, with the full supportability based on the robust County network architecture and NetBond connectivity to the O365 cloud tenant, facilitating quality of service and performance. This standard will not integrate outside agencies, which use non-Skype for Business room systems; however, Microsoft is currently developing a cloud MCU that will be hosted in the Azure cloud and will offer interoperability with disparate systems scheduled for availability later in 2016.

As mentioned earlier, a resource unit standard will be maintained for larger collaboration spaces and meeting rooms around the County. These locations can benefit from increased collaboration capabilities, including multi-touch displays, digital whiteboard capability, HD cameras, and integrated Windows OS. These capabilities are available in a variety of size options beginning at 55" and going as large as multiple 70"+ screens, which are capable of not only allowing for full video conferencing via Skype for Business, but also have native Microsoft Office support to allow for the display, edit, and sharing of all forms of content. These displays have the capability to be wall mounted or mounted on a rolling stand and use an integrated Android implementation as the panel control system while leveraging a licensed Windows 10 system on a chip, which is capable of being centrally managed and patched via SCCM. A unique account will be created in Active Directory, which is used to identify and "log the system in." This account will be allocated as a resource and will be available to be scheduled in the County's exchange environment. Figure 74 presents Microsoft Surface conferencing systems and features.

Figure 74. Touch Screen-Based Conferencing



Examples of touch screen-based Microsoft Surface conferencing systems.

Video Streaming and Archiving Services (Sched. 4.3, Section 5.10)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

To support the increasing video distribution needs of the County, from both live and on-demand perspectives, our proposed near-term solution uses the existing Granicus System as a compliant starting point. This provides continuity and stability as more future-focused technologies are investigated.

Although the current solution for video streaming and archiving sufficiently supports internal and external video for events such as Board of Supervisors meetings, our team recognizes the potential in using the same video on demand and streaming strategies for training and Town Hall purposes as well. New solutions would allow the County's staff access to training and presentations while in the office and via mobile devices.

We have determined that the best way to move forward in transforming video streaming services is to engage in collaborative discussions regarding the County's objectives for internal and external content distribution. These interactions are critical in developing our overall transformational approach and have proven beneficial in past successful advancements. This interaction will allow our team to better

understand the County's needs and will provide the forum to talk about features and capabilities that may provide added benefits from a business and community support perspective. Accordingly, our SMEs will discuss technical capabilities and potential use cases with the County personnel and collect their critical input, allowing us to articulate recommendations that support the near-term requirements and posture the County to achieve longer-term objectives more effectively.

Although our team is recommending continued use of the existing Granicus solution, it may not meet future requirements in an efficient manner. The current archived content is hosted in the cloud, and as internal users access and view this external content each connection is brought in through the firewalls and Internet connections to reach the intranet user. As the number of these connections increase, the overall available Internet bandwidth decreases. As such, our solution must recognize the need to add Layer 2 Internet Group Management Protocol (IGMP) snooping and Layer 3 multi-cast support via Protocol Independent Multicast (PIM), as well as Content Delivery Network (CDN) capabilities at both the COC and AT&T POP.

As our SMEs review potential long-term solutions to deal with these issues, we will bring forward leading industry solutions for consideration. Options include the expanded use of existing Akamai capabilities as well as other solutions, such as AT&T Video Management Services (AVMS) with Qumu, which could be evaluated for deployment. Alternatively, a review of the current offerings available with the Granicus service presently used by the County may reveal potential features for County consideration.

Our team's close collaboration with the CTO and other stakeholders allows evaluation of the features and implementation options such as these to move forward, while matching those capabilities to the business needs of the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

In meeting the video streaming and archiving requirements, our approach uses the two current core facilities already in use at the AT&T POP as well as the CAC as a primary video content sourcing location. Furthermore, this solution uses the existing network infrastructure to support an efficient video distribution capability. Our local, dedicated staff will be active liaisons on behalf of the County, and we will select external cloud providers so that required service level requirements are continually met.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The key to our success on behalf of the County is our trusted working relationship with County personnel. Going forward, we will achieve consensus on the Video Streaming and Archiving Services Roadmap by vetting or via recommendations in the weekly network architecture meetings—and thereafter via the Enterprise Architecture Forum. Use of these iterative processes allows our solution to address known and projected business requirements, convey direction, gain insight regarding other project path implementations, and allow required approvals while maintaining consensus. As such, our SMEs will continue their active participation within these forums as well as their participation in other meetings to stay abreast of customer needs, report on changes in technology, and propose low-risk solutions to meet County business requirements. Furthermore, our team uses insight gained from the ongoing operational and maintenance aspects of the infrastructure to assess potential transformational, refresh, and upgrade opportunities. For instance, based on further analysis of the Granicus implementation, if single points of failure are identified and can be remediated then our SMEs understand the processes and documentation to effect the change with minimal effort by all parties involved. Our local, dedicated team provides the coordination of resources necessary to plan, design, and implement the video and archiving solution. All work efforts and problem reports would flow through the existing processes in place for support of the County's network by the AT&T LCM team.

On a continual basis we will create, maintain, and update end-user training documentation and tips, as well as associated help desk scripts pertaining to the proposed solution, to match the version and features of the product.

- Automated Tools – Automated systems and tools involved in proposed solution

As new appliances and capabilities are expanded within the existing data network, our team will also expand the use of CA Spectrum and eHealth to monitor the operational status of the appliances and the bandwidth usage so that the ongoing operational capabilities are met as compared to the service level requirements. High-grade analytics provide viewer statistics along with performance information to provide a clear picture of performance and where possible trouble spots within the infrastructure may be occurring so that we can take near-real-time corrective actions.

- Qualifications and Experience – Background and experience in comparable environments

By drawing on the qualifications and experience of our local, on-site team in conjunction with cloud-based resource support staff, the County gains industry best resources for the achievement of service level requirements.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

See Volume 2.08.1, Section 2.8.8, where we describe our approach to the Town Hall video.

Mobility Infrastructure Services (Sched. 4.3, Section 5.11)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Through collaboration with the County's Chief Technology Office as well as Group IT and department managers, AT&T has designed, delivered, and implemented a fully operational Enterprise Mobility Management Infrastructure suite that meets all of the stated requirements within the new Contract. This platform was implemented in 2014 and has been a catalyst to the mobilization of County users and business processes, enabling new use cases and creating value across the enterprise.

AirWatch MDM Infrastructure

All components of our industry-leading AirWatch Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for the County are implemented in a fully geo-redundant configuration. The AT&T MDM solution uses a cloud-based AirWatch Software as a Service (SaaS) MDM/EMM solution integrated with on premise AirWatch Cloud Connectors (ACCs) deployed into the AT&T POP and the County Operation Center. These ACCs in turn interoperate with the County's Active Directory infrastructure for user authentication.

Another aspect of our comprehensive solution is our proxy services between County Enterprise Systems and the SaaS MDM/EMM cloud, as well as application gateways services for developed or acquired applications, to internal County resources from mobile devices using Mobility Infrastructure Services. For example, the Mobile Access Gateways (MAGs) located at the AT&T POP and at the County Operations Center provide access to user mobile devices using the AirWatch Secure Browser and the AirWatch Secure Content Locker mobile application, which are offered in the County mobile application store. Figure 75 below depicts the AirWatch premises-based infrastructure.

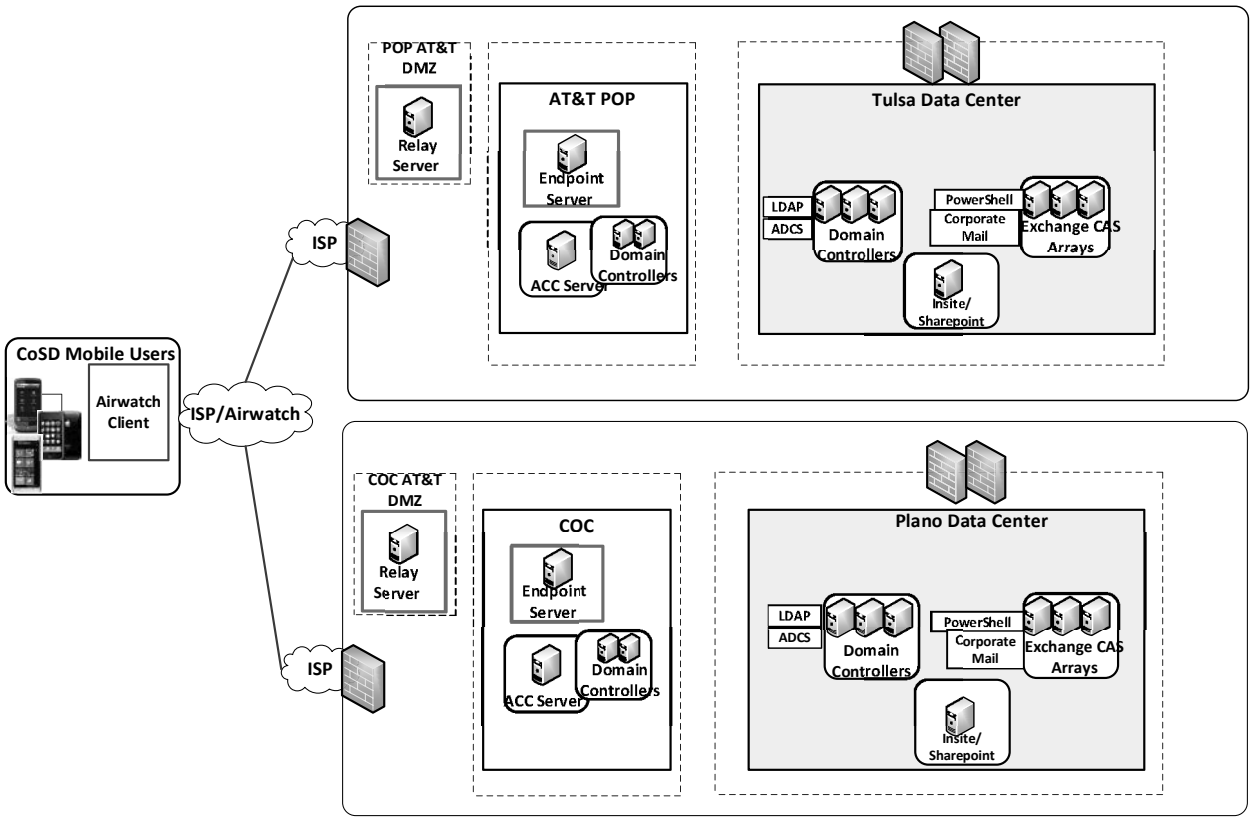
Due to the nature of the cloud service and the geo-redundant configuration of the on premise infrastructure, the AT&T MDM solution has no identified single points of failure.

Mobile User and Device Profiles

At present there are three profile groups established within AD, and these are the Corporate Single Device, the Corporate Multi Device, and the Bring Your Own Device (BYOD). These profile groups can be expanded as business needs are defined, where our team simply adds a group profile within AD recognized by the AirWatch Platform. Users are identified through CSRFs and placed into the respective groups.

Our deployed solution supports County "corporate owned" devices and BYOD in a reliable and secure manner and manages them according to specific County-defined policy.

Figure 75. AirWatch



The AirWatch premises-based infrastructure offers geo-redundant, high-availability services for connectivity to the enterprise.

Although the current difference between County devices and BYODs is that County devices have access to the County mobile application store, future business decisions may expand these differences. After being enrolled within the designated group, when a mobile device user requests access to the County domain, the user is certified against the AD; thereafter three profiles (Passcode, Restrictions, and Exchange) are pushed Over the Air (OTA) to the device.

The AirWatch cloud-based solution provides central management and control of all mobile devices and mobile applications from a single unified console. This console also allows our solution to enforce County-approved device policies for security and data protection across the user population of County

and BYOD mobile devices. For instance, our solution provides the County Mobile Application Store for developed or acquired mobile applications and limits the access to the applications to only County-managed MDM devices.

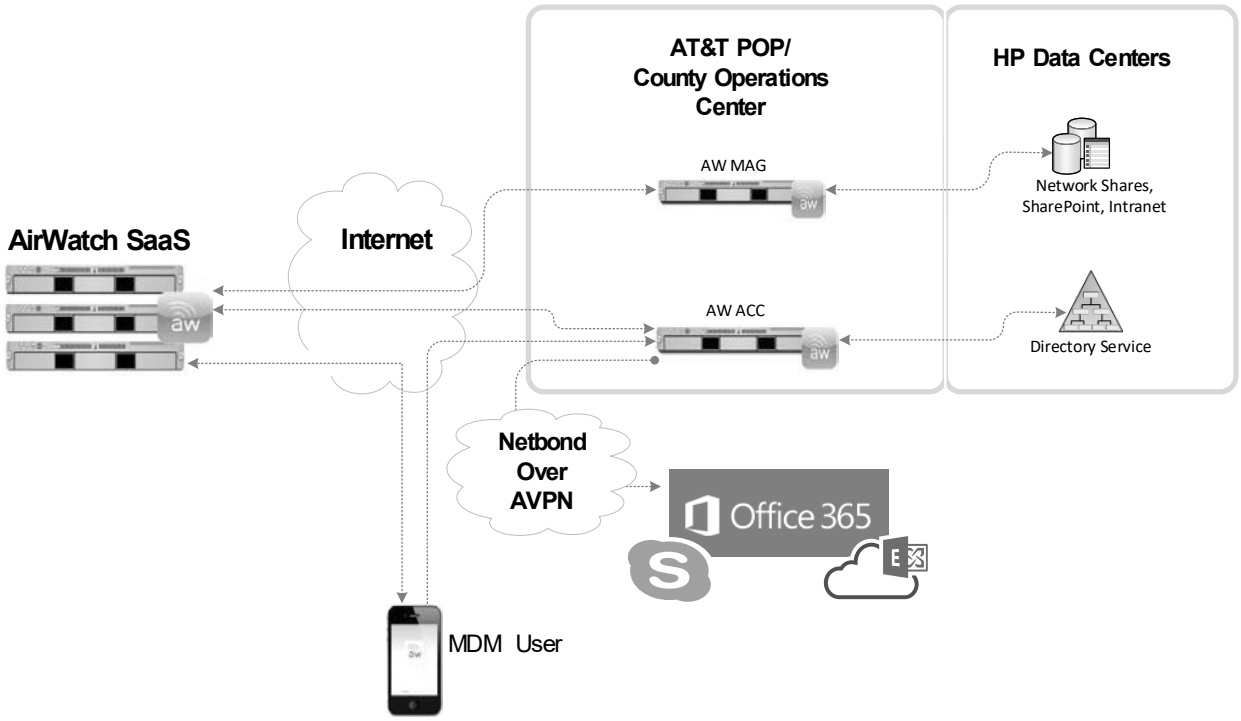
Mobile User and Device Authentication

AT&T enables client authentication, encryption, and message signatures to secure corporate resources and connections. AT&T's SaaS MDM/EMM solution integrates with third-party Certificate Authorities and Public Key Infrastructure (PKI) providers in cloud and on premise deployment models. AT&T's SaaS MDM/EMM solution will be distributing Symantec Managed PKI certificates to corporate managed mobile devices for mobile VPN authentication and integration. Future roadmap capabilities include the potential for PKI integration delivered via AirWatch MDM for access to County staff Wi-Fi as well as seamless integration with the PulseSecure Mobile VPN application.

AirWatch Integration with O365

As a transformation initiative, HPES plans to migrate Exchange to the O365 cloud. Although the current integration from the AirWatch SaaS MDM/EMM solution to the County infrastructure for email services is premises based with integration to services in the data center, the solution can be configured to integrate to Office 365 with Outlook via an AVPN with AT&T NetBond service. AT&T and its Mobility Solution Services team will engage in this migration effort, updating design documentation and making certain that user connectivity to email is enabled as the services are migrated to the cloud. Figure 76 presents the reconfiguration of the AirWatch premise-based infrastructure.

Figure 76. AirWatch



The AirWatch premise-based infrastructure will be reconfigured as part of the migration of Exchange to the O365 cloud, enabling email access to MDM-compliant devices.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

We will use the existing, knowledgeable AT&T Lifecycle Management team located at 7337 Trade Street in San Diego, California, along with AT&T's leveraged Mobility Support Services (MSS)/Application Service Desk (ASD) organization to continue to support the premise- and cloud-based AirWatch infrastructure.

The ASD is composed of experienced, industry-certified professionals who provide hands-on, comprehensive, and proactive managed services and technical support. In addition to the ASD, the local team also retains a highly skilled mobility consultant, who has intimate knowledge of the County AirWatch tenant and continually provides support and guidance on operational and strategic initiatives.

Facilities involved include an AT&T POP in the County as well as the County's Operations Center.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The SaaS MDM/EDM solution is installed and is in place today. Key processes include the following:

- User acquires phone and needs access to County resources.
- A request is made for access via an Install/Move/Add/Remove (IMAR) through our help desk.
- User goes to the public apps store and downloads the MDM/EDM application.
- Our team processes the request and gives permissions for allowed systems for the user.
- User enrolls into the MDM/EDM system via a user guide provided by our team.
- Any issues are directed to the help desk.

Our MDM service includes upfront perpetual licensing costs which are proposed as an OIC purchase at the time a new user subscribes to the service. This license cost is one time and is separate from the monthly RU. The one-time license price is normalized based on the existing user base and the potential for re-use of licenses freed up by users that unsubscribe from the service.

Our mobility infrastructure SMEs play an integral role as trusted advisors within the Enterprise Architecture Committee as well as outside the forum. During the current Contract and into the new Agreement, our staff will participate as dedicated resources supporting upgrades, refresh, and transformational activities related to mobile infrastructure services. Our SMEs will continue to use Pilot Charter and Solution Design Documents as well as other documents and briefings to convey our recommendations for County review.

Through our ongoing work with evolving technologies and technology vendors, we recognize that the technical landscape is changing rapidly. To stay up to date we recommend quarterly collaborative reviews of mobile device standards, including hardware and operating systems, for incorporation into the County Standards and Procedures Manual for Standard Mobile Devices. Furthermore, our team will use the approved County manual when developing standards for all mobility infrastructure services that are submitted for approval on a semi-annual basis because these service platforms must maintain interoperability. Although the mobile infrastructure hardware and software service components are on a 4-year technology refresh cycle, we also recommend quarterly updates to the timeline/roadmap of all mobility infrastructure services hardware and software version life cycles so that responsive time frames and completion dates stay within supported versions of hardware and software.

Our interactions within the EA meetings and related support activities result in our staff posting artifacts relating to mobility infrastructure services into the Service Portal. Documents such as the Pilot Charters and SDDs are located within appropriately restricted Service Portal locations, and detailed user instructional documents for Tier 0 support are posted within other areas of the Service Portal for general

access. To further enhance our user support, we recommend short instructional videos and self-help tutorials for basic user education. These short videos walk users through numerous aspects regarding configuration and the use of their mobile devices.

- Automated Tools – Automated systems and tools involved in proposed solution

Our AirWatch MDM solution offers the County a centralized dashboard to enforce policies, set restrictions, and secure devices while in use, lost, or stolen. The dashboard offers a single console to monitor all mobile device activity, lock and wipe devices, set privacy policies, update profiles, and re-provision devices. Our team uses this console to monitor user compliance with County policies.

- Qualifications and Experience – Background and experience in comparable environments

Currently, AT&T provides this service to the County with local AT&T resources and an extended managed services support team. Local AT&T resource accreditations include:

- AirWatch Enterprise Associate
- AirWatch Enterprise Professional.

Our local technical team retains, at its disposal, a deep bench of subject matter experts who have the expertise and experience to handle any new transformative or operational objective or issue. While delivering world-class support of the existing technology base, this pool of resources has depth and breadth of knowledge that allows the team to analyze alternative technological/process options and support changing business needs.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Wireless Network Access Services (Sched. 4.3, Section 5.12)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Our approach to enterprise wireless service focuses on providing high performance, scalability, security, and ease of access for County staff users and the public. Over the life of the existing Contract the County's wireless network has grown by more than 30% per year, and our expectation is that this growth trajectory will continue in the coming years as the County continues to increase the density of its wireless footprint.

Our team designed, implemented, and currently manages a comprehensive wireless architecture that provides services to County staff and constituents. Our solution provides wireless services for managed computing assets on the secured County internal wireless LAN as well constituent and guest assets on a public Wi-Fi infrastructure. This wireless infrastructure consists of centralized geo-redundant controllers, wireless access points, various software-based management tools, and security components.

Wireless Infrastructure

At the core of our solution our two centralized wireless LAN controllers provide redundancy and resiliency through high-availability, geo-redundant configurations that leverage diverse facilities (AT&T POP and the County Operations Center). These controllers maintain our centralized configuration, act as a

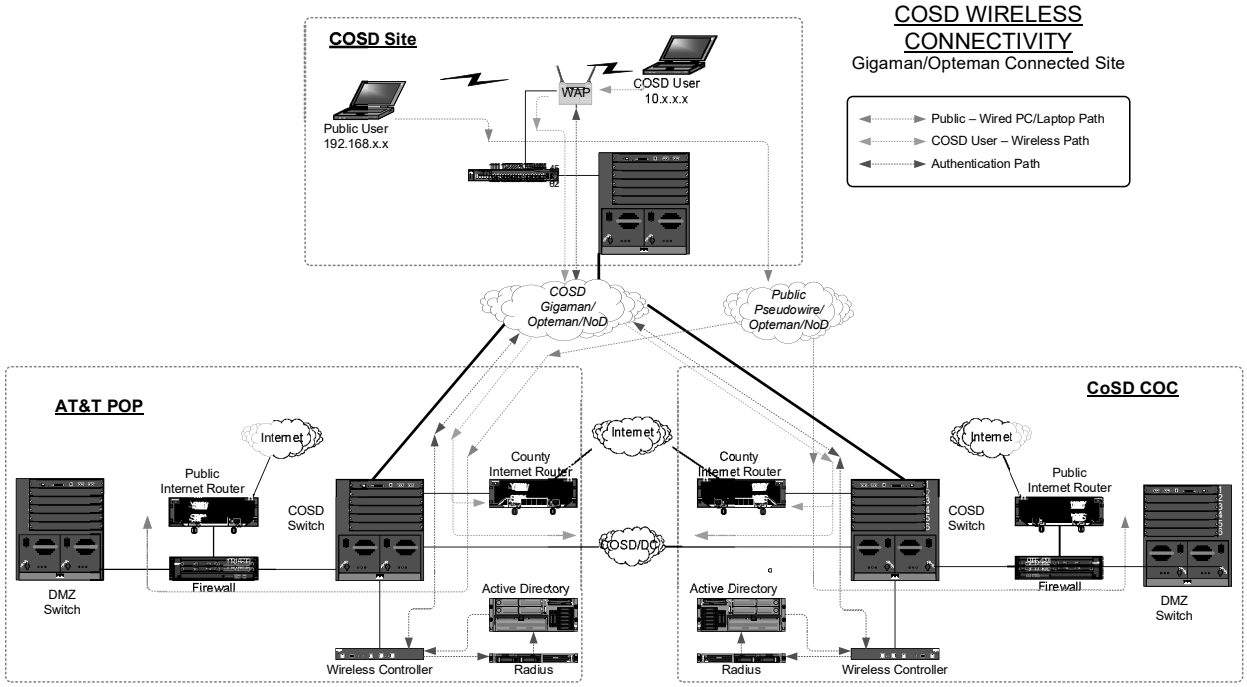
single point of interface for changes and monitoring, and support a variety of access point models. Figure 77 details the County's geo-redundant wireless controller infrastructure.

Today more than 380 wireless access points throughout the County provide wireless connectivity for the end user. These access points are a mix of Cisco and Aruba hardware dependent on the specific application. Our team has standardized on the Cisco 3702 for wireless access within County facilities, whereas for outdoor areas we have standardized on the Aruba 274/5. Both products provide support for legacy connectivity, such as 802.11 A/B/G/N as well as the new 802.11AC standard. This wide range of support allows all Wi-Fi capable devices, regardless of age, to obtain connectivity through the County wireless infrastructure.

Our team has conducted two early refresh activities over the life of the current Agreement so that the County has the latest high-performance solution available for new use cases as the industry evolves. The County's requirement to refresh Wi-Fi on a 36-month cycle is an appropriate timeline given the advancements expected in the coming years.

Our team uses several software suites to provide visibility deep into the operations, planning, and support of the County's wireless infrastructure. These tools include management tools, such as Airwave and Cisco Prime Infrastructure, as well as survey tools such as Fluke's Air Magnet.

Figure 77. Geo-redundant Wireless Controller Infrastructure



The County's geo-redundant wireless controller infrastructure supports dynamic failover of staff and public wireless services between diverse core facilities.

Wireless Network Authentication

For County secure wireless, our team has worked with desktop support services at HPES to deliver a certificate to all managed devices required to authenticate via EAP–TLS and connect to the County's secure wireless infrastructure. Public access is also provided in various County locations, such as the libraries, and is segregated logically and physically. Additionally, we use our next-generation firewall

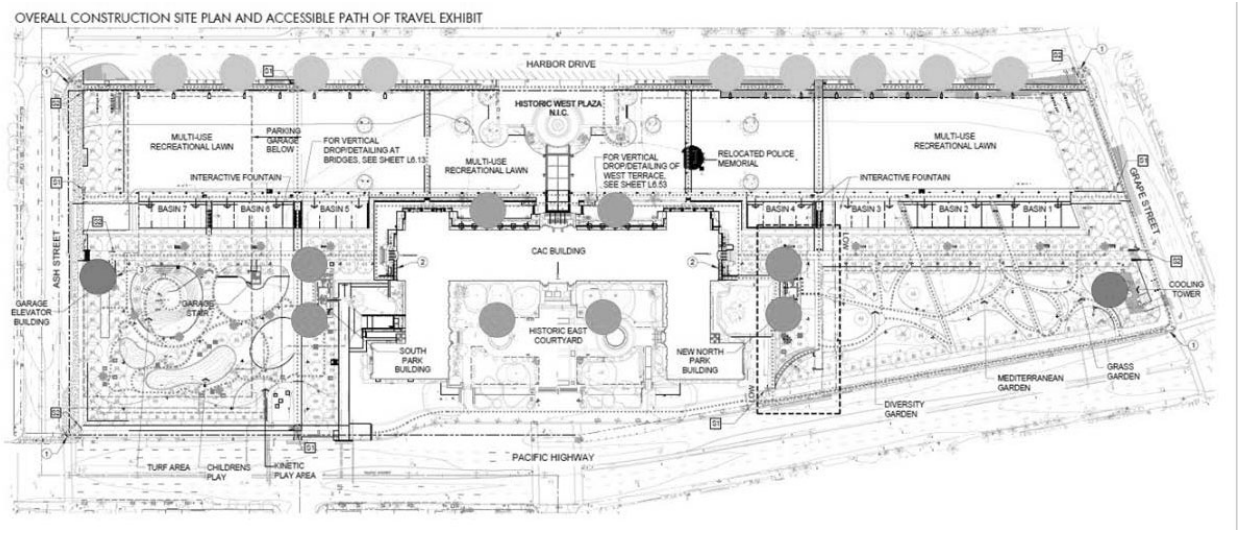
infrastructure, including content filtering functionality, to provide the most robust security available for the wireless infrastructure.

This architecture, coupled with an NAC and PKI initiative, will serve to further increase the security posture of the wireless infrastructure. By leveraging these capabilities additional controls will be enabled, providing seamless access to wireless staff users, while redirecting untrusted/unmanaged assets to a guest access portal via a splash screen, where they can then obtain public network connectivity. This architecture supports a closed loop system whereby only known, managed assets are able to connect to the secure wireless infrastructure, with little to no additional interaction from the users to facilitate this additional security. For more information on NAC and PKI based wireless authentication, please see Volume 2, 2.08.01, Section 2.8.9.

Outdoor Wireless Deployments

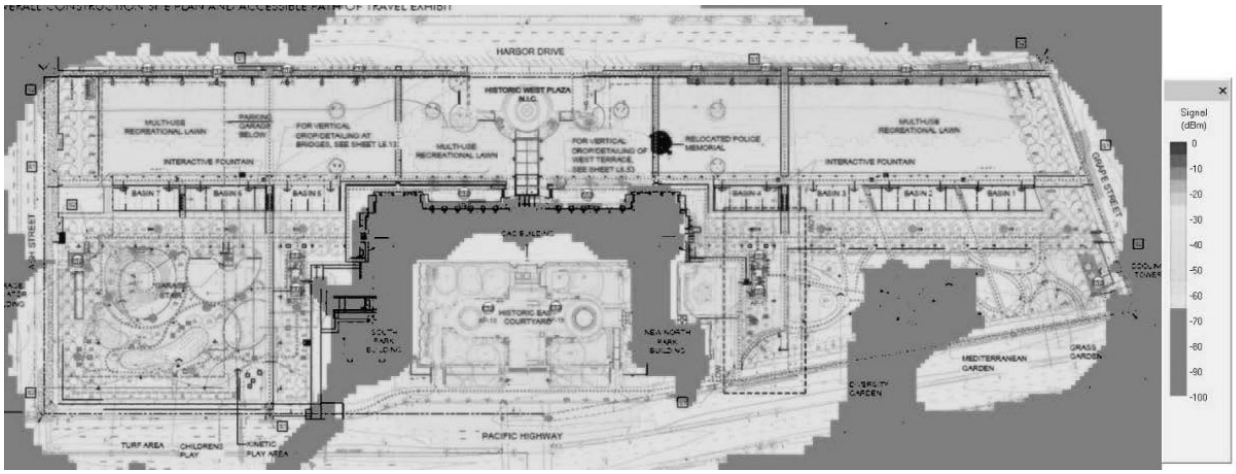
In 2015 our team proactively developed a proposed design for outdoor wireless coverage at the County's Waterfront Park (Figure 78 and Figure 79). This design included an in-depth analysis of the radio frequency (RF) environment to provide a comprehensive and detailed view of the environment and articulate obstacles that might hinder operation. Our proposal was evaluated by the Land Use and Environmental group and was partially implemented to provide a subset of coverage in and around the Snack Shack with the potential to implement the full design at a later time. Through this development process we established a new outdoor wireless access point standard and began looking at use cases that could be used elsewhere across the County. This proactive effort has since led to an increase in outdoor Wi-Fi deployment at County parks as they begin building on the business case for offering Internet access to park patrons.

Figure 78. County Administration Center Waterfront Park



The County Administration Center Waterfront Park wireless survey proposed a wireless deployment that provides coverage across the entire grounds. This design was partially implemented.

Figure 79. Wireless Survey Tools



Our wireless survey tools can effectively project the footprint of wireless surveys across an architectural drawing of the facility.

Ubiquitous Wireless Deployments

As Wi-Fi services adoption continues to increase, we recommend that the County shift its focus to a high-density client coverage model that focuses ubiquitous accessibility. To date, business units have deployed wireless access points only in selected work areas within certain facilities, creating "hot spots" within these locations. This creates a situation where users at the edge of these zones are slowing the throughput of the wireless access points and other users' wireless access. This is due to the throughput dynamic of the wireless access point as it takes into account the physical distance of the clients from the access points, volume from the number of clients connected to each access point, and the utilization of legacy protocols, such as 802.11B/G. To provide a more consistent, high-performance wireless experience, we recommend that business units increase density within their facilities. A ubiquitous wireless footprint in County facilities would enable the workforce to move throughout the site without deviations in speed or connectivity and would provide long-term positioning for advances in wireless communication (such as Voice over Wi-Fi [VoWiFi]), which can leverage emerging standards, such as 802.11AC Wave 2 and Wave 3. These types of advancements are expected to eventually eliminate the need for wired infrastructure for many managed computing devices entirely because the speeds and throughput will surpass that of current wired connection in the County, which is 1 Gbps.

Our proposal encourages increased wireless density through aggressive price banding in the wireless RU's. Although some facilities may not have a specific need for a ubiquitous wireless footprint, the larger County sites (particularly those with shared, multi-department/business unit workspaces) would benefit greatly from the increased density. We plan to work closely with the IT contacts at these locations to conduct wireless surveys that would provide a clear picture of the number of wireless access points required to provide full coverage at a given site. This would allow departments and business units to determine their allocation of the RU cost based on the number of active users at the facility.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The local, dedicated LCM team provides all design, implementation, support, monitoring, and reporting of all wireless network services.

Core infrastructure for the wireless network is housed at the AT&T POP and County Operations Center, which provides secure, restricted access. Wireless access points are installed upon request in County facilities according to industry and County-approved standards.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Our engineering team works with County's CTO to evaluate the new and emerging wireless standards and their enterprise readiness. Our recommendations take into account not just the performance of new wireless access points, but also the device standards being used by County end users, so that the timing of the investment enables the largest population of users to take advantage of the advancements.

When a recommendation is approved, our team moves forward with project management processes, including planning, scheduling, and implementation of the refresh of existing equipment as well as other infrastructure changes.

For equipment issues, our help desk and engineering team work to identify and remediate the problem.

- Automated Tools – Automated systems and tools involved in proposed solution

Tools include management, operation, capacity/performance, and monitoring. Some of these tools include Cisco Prime Infrastructure, Wireless Control System (WCS), AirWave, Spectrum, and eHealth. We use these tools to measure and take action to maximize performance of the network, as well as to provide ongoing reporting.

- Qualifications and Experience – Background and experience in comparable environments

Our team has designed, implemented, and supported the County wireless network for more than 9 years. We have effectively managed the environment and made recommendations for improvements, including the elimination of single points of failure.

Our personnel undergo ongoing technical/product training, including industry and manufacturer certifications and continuing education.

Our team holds the following certifications in the wireless field:

- Cisco Certified Network Associate – Wireless
- Cisco Certified Network Professional – Wireless
- Certified Wireless Network Professional (CWNP)
- Global Information Assurance Certification Auditing Wireless Networks (GIAC GAWN)
- Aruba Certified Mobility Associate.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Third-Party Network Access Services (Sched. 4.3, Section 5.13)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Our team's proposed solution for third-party network access uses the existing solution sets developed over the life of the current Agreement in response to expanding business requirements to support third-party access to and from and across the County data network. Overall, there are three different types of support required:

- Dedicated leased line connectivity
- IPSec connectivity
- Virtual circuit support.

Each of these solution sets play a vital and specific role in supporting various County business areas. The solution used for access is based on the location of the third-party devices, the type of communication required (system-to-system versus user interactive session), the tolerance of bandwidth variations, and latency impacts.

The County's Building Automation System (BAS) solution is a perfect example of our third-party access technology in use. The BAS devices at almost two dozen different County locations are able to communicate among themselves and their centralized management servers, without having direct access to the County network as a whole. This allows for the best vendor solution to be used without posing undue exposure of critical systems and assets.

Using the Third-Party Access Request (TPAR) process, we determine the required connection types and any details necessary to provision the access. This process identifies the specific third-party devices, the County resources being accessed, and whether the communications occurs over the internal domain and/or open Internet. This information is used to create strict firewall policies so that only the approved devices and resources are accessed for use by the third parties.

The County's existing unified threat management technologies provide intrusion detection and prevention, virus and malware filtering, firewall security policies, monitoring, and reporting for these third-party connections. All data traverses the County's next-generation firewalls to enable full visibility into all data flows up to and including the application level. All data classified as sensitive and above must be encapsulated in a secure tunnel as it egresses the County network, regardless of its point of origin within the managed network.

Third-party interfaces are also included in the LCM team's capacity and performance monitoring services. This approach facilitates reporting on usage and possible impacts to performance resulting from spikes or increases in usage. All access to County resources from third-party users is managed via Active Directory and user account levels of access.

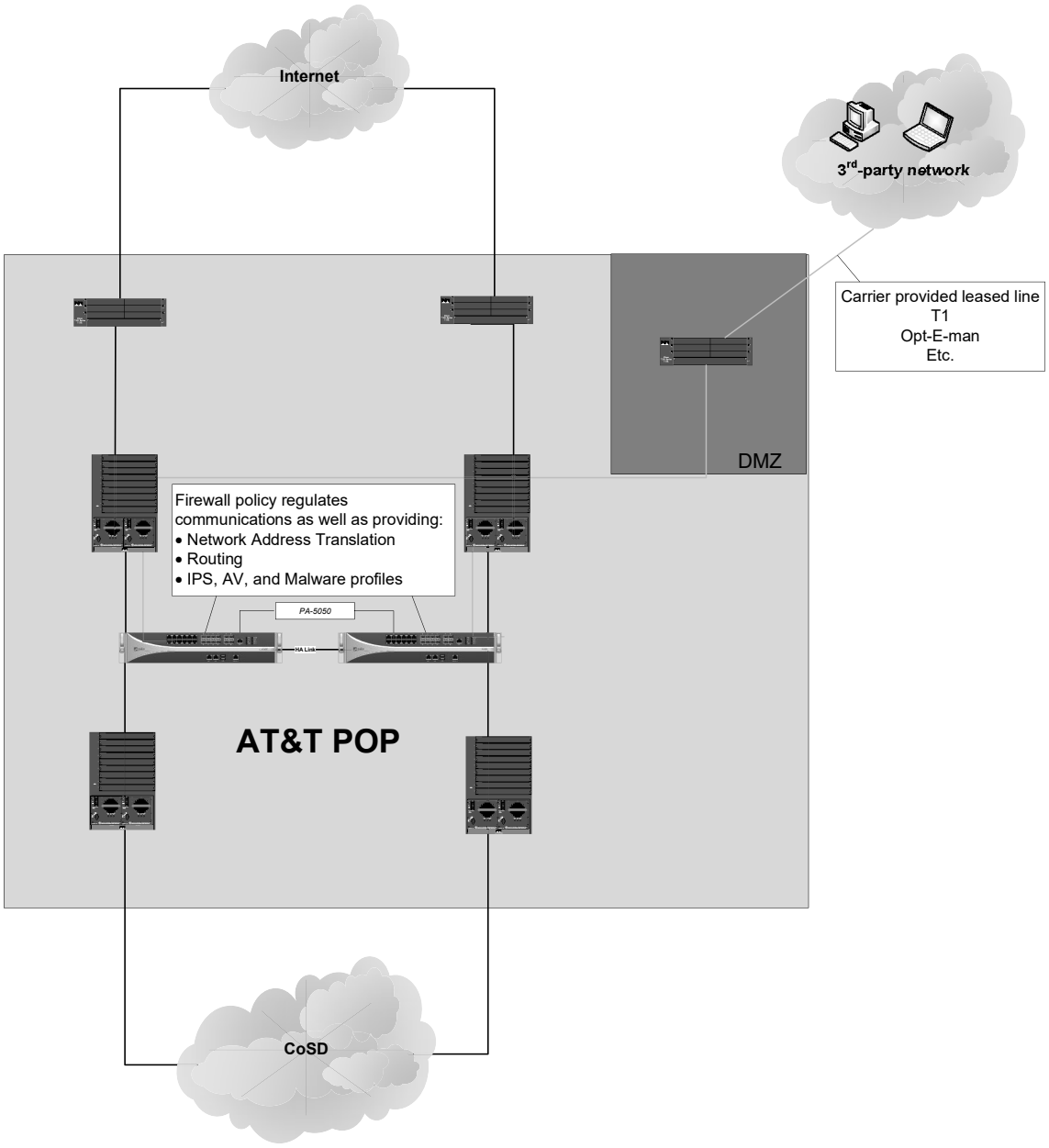
The third-party network access models and use cases are as follows:

- **Dedicated Leased Line Connections.** Third-party leased line connections are used to connect the County network to a third-party network via a dedicated transport (i.e., T1, Opt-E-MAN, Opt-E-WAN, and so forth) that is provided by the third party. This solution is chosen when throughput must be guaranteed because the dedicated circuit is not impacted by fluctuation in utilization of public Internet circuits. A dedicated circuit also provides the highest level of security in terms of confidentiality, integrity, and availability. Figure 80 illustrates the connectivity of a leased line connection into the DMZ prior to traversing the firewalls to gain access to the County-designated resource.
- **IPSec Connections.** IPSec provides a secure tunneled connection over the Internet. It encrypts sensitive data and allows machine-to-machine connectivity for scenarios where automated jobs run

connections into or out of the County network without user interaction. It also provides access into the County network for authorized systems or users without the need to install specialized VPN software on the remote hosts. Figure 81 details IPSec third-party connectivity design.

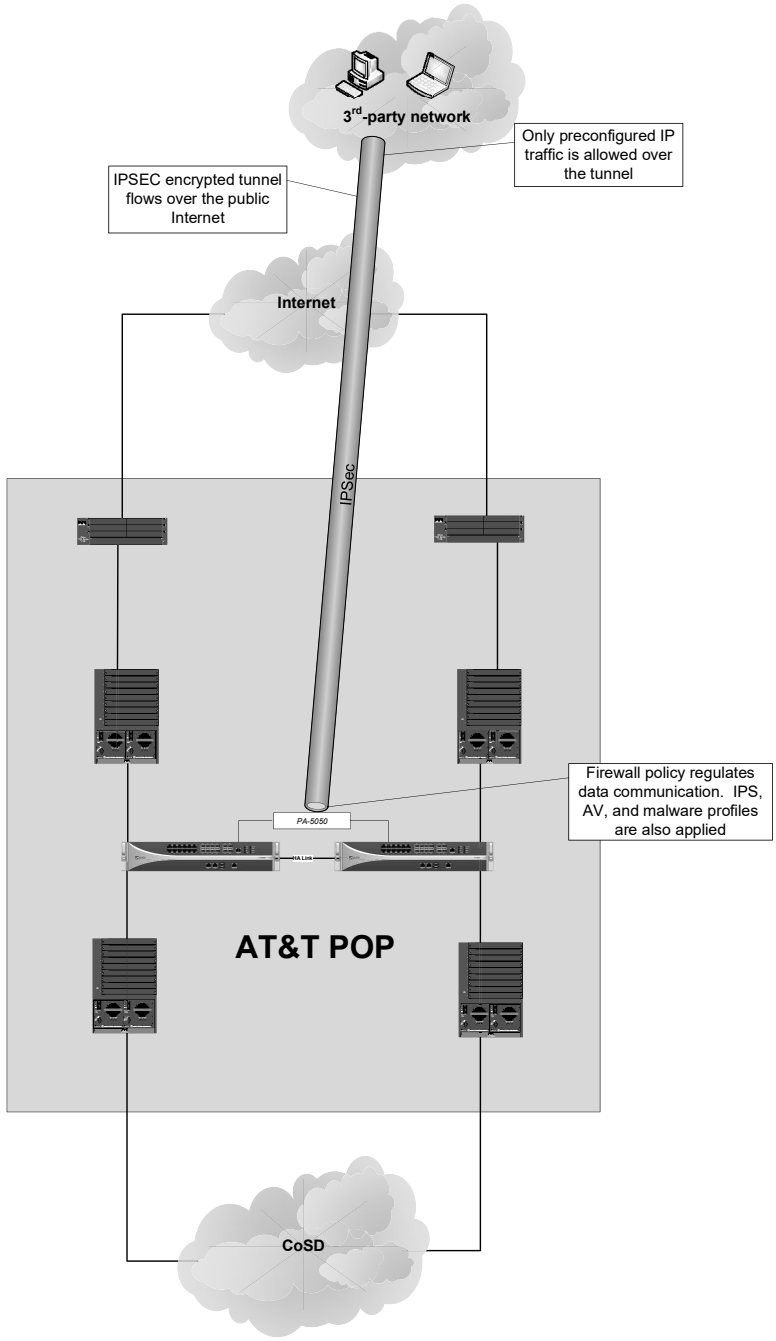
- **Virtual Circuits.** The virtual circuit design allows placement of non-County devices onto the County network in a way that keeps them isolated from County assets. All communication to and from County resources is still regulated by firewall policies. Presently, this solution supports users within 55 virtual circuits inside the County domain without exposing the network to risk. Figure 82 presents virtual circuit third-party connectivity design.

Figure 80. Leased Lines Third-Party Connectivity Design



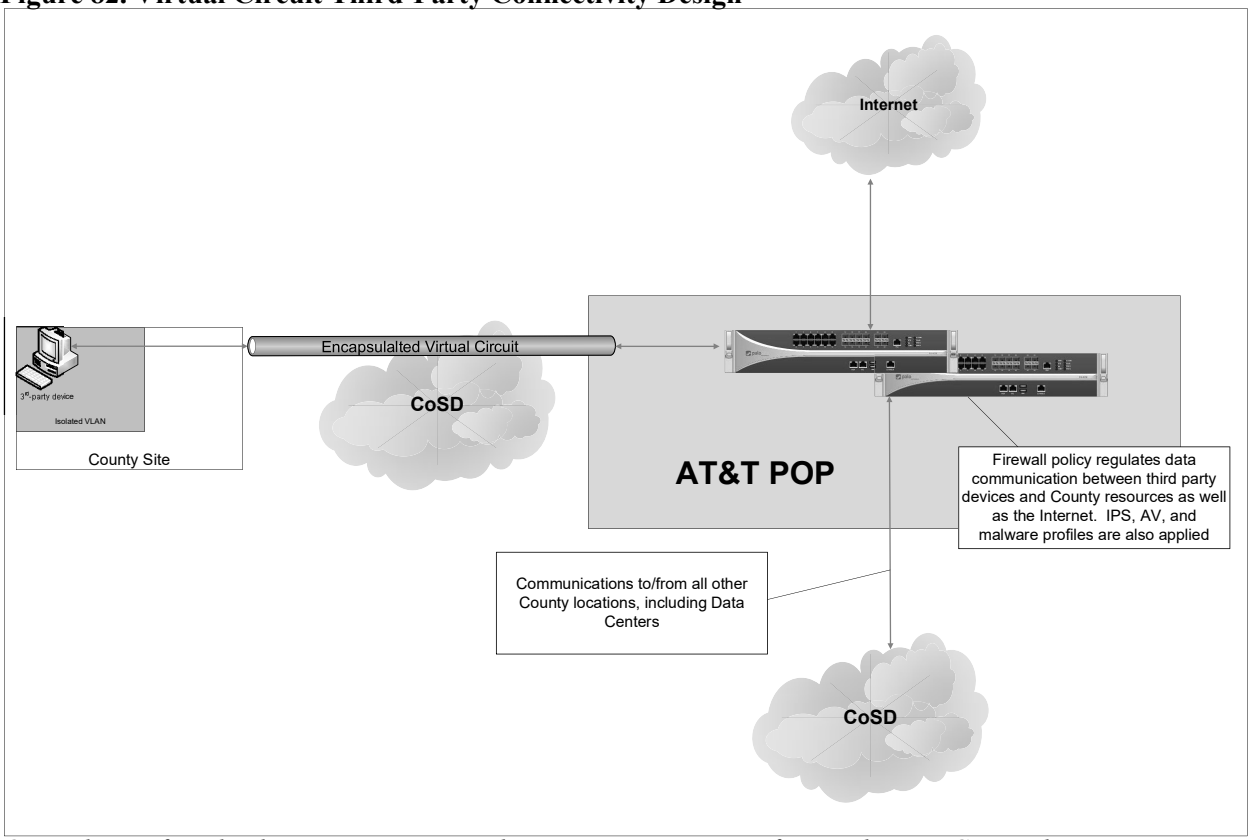
Our solution for Third Party access provides secure connectivity for conducting County business.

Figure 81. IPSec Third-Party Connectivity Design



Our solution for Third Party access provides secure connectivity for conducting County business.

Figure 82. Virtual Circuit Third-Party Connectivity Design



Our solution for Third Party access provides secure connectivity for conducting County business.

As part of the dedicated team's ongoing efforts to provide continuous improvements to, and enhancements of, all frameworks for which they are responsible, we are continually looking for alternative solutions that will benefit the County's voice and data network. As such, a transformative approach to IPSec third-party access is available and recommended by AT&T, whereby third-party services can leverage the geo-redundant ISP links. This solution would allow adopting third parties to create a second, dynamic peering relationship with the County Operations Center ISP link, enabling failover in the event of a service disruption.

We are also looking into the feasibility of leveraging the AVPN solution to provide redundancy for those groups using leased line connections.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The local, dedicated LCM team provides all design, implementation, support, monitoring, and reporting of each of the third-party access solutions. All managed hardware in association with such is housed at the AT&T POP, which provides secure, restricted access as well as fully redundant power. Technical personnel and hardware associated with the County program are dedicated to the program.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The local, dedicated LCM team is embedded in the full life cycle of every third-party access connection—from the initial gathering of requirements, through the design and implementation phases, to managing and monitoring, and even decommissioning when requested. Through customer meetings and

security reviews, the team evaluates the proper access method so that it is sized appropriately and verifies that all necessary security measures are in place.

Third-party network access options are continually evaluated based on County business requirements in addition to current and emerging technologies.

The current solution represents the best approaches available for meeting each of the specific requirements for supporting County business in connection with third-party access. However, as technology evolves and the needs of the County change, we will change the solutions to adapt accordingly to best meet those requirements.

- Automated Tools – Automated systems and tools involved in proposed solution

In our solution automated monitoring is in place for the notification of any hardware failure or fault for these third-party connections using the CA Spectrum platform. Our solution also proposes monitoring utilization to allow for capacity and performance reporting and planning using the CA eHealth toolset. Alerting based on IPS/IDS, AV, and malware protection is also set up for immediate response and remediation of any threats posed to the County network by third-party devices or users.

- Qualifications and Experience – Background and experience in comparable environments

The LCM team dedicated to the County program consists of network and security engineers who have decades of combined experience in designing, implementing, and supporting these specific solutions and an average of 9 years of experience directly supporting the County. The LCM team's knowledge of the solution and the County customer maximizes the County's return on investment while minimizing transitional risk.

As needed, the local technical team retains, at its disposal, a deep bench of subject matter experts who have the expertise and experience to handle any new transformative or operational objective or issue. This pool of resources has the depth and breadth of knowledge that allows the team to analyze alternative technological process options and provide that information to the County for their evaluation.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

External DNS Management Services (Sched. 4.3, Section 5.14)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

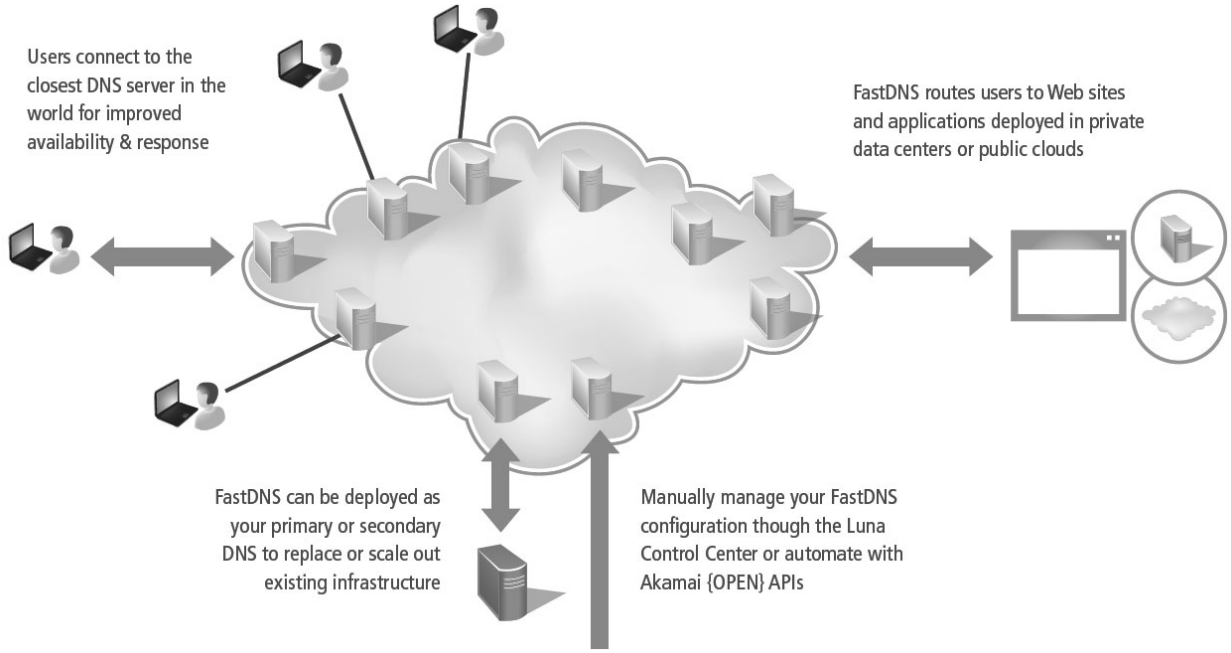
In mid-2015 our team worked with the County to re-architect and migrate external Domain Name Service (DNS) to a scalable, redundant, and fault-tolerant cloud-based platform. This recently implemented solution, using Akamai cloud-based FastDNS service, will be the basis for our DNS management service as provided in the new Contract term.

The Akamai FastDNS solution provides an authoritative DNS service that offloads DNS resolution from the County's infrastructure to the cloud to provide 24x7 DNS availability. It is optimized for performance through global distribution and presence and reliability—protecting against DDoS attacks while allowing for additional security through the Domain Name System Security Extensions (DNSSEC) to protect

against DNS forgery and manipulation. Our team will perform DNS management as required for all of the external-facing County DNS records (A, MX, CName, and so forth) via a web browser that accesses the Luna Control Center. The Luna Control Center is the web-based portal that provides customers with access to—and control of—their Akamai services as well as reporting and monitoring functionality.

Through coordination with the County, we will be provided with requests to add, move, or change the information published for specific domain name records within the Akamai solution, as well as remove obsolete records to preclude any instances of orphaned or bad records. Although the existing DNS implementations allow a logical separation between the internal and external DNS, our SMEs can integrate specific elements, as required by the County, subject to essential network security provisions. Figure 83 illustrates Akamai FastDNS service.

Figure 83. Akamai Fast DNS Services



Akamai FastDNS service provides redundant, cloud-based DNS services through the Luna Control Center web portal, allowing rapid deployment of changes to the entire Akamai hosted DNS infrastructure.

As trusted advisors to the County, our team is a fully immersed group of architecture and management resources that participate in the planning of upgrades, refresh, and transformational activities related to external DNS management services. A key activity includes the continual process and implementation improvements needed for support within the service level requirements. For instance, the present external DNS solution was deployed as a value add on an already geo-redundant, high-availability solution. After discussion with the County, it was determined that there was an opportunity to leverage existing investment made in the Akamai cloud for dynamic web hosting, and our team agreed to simply redefine the process by which we manage DNS to use the new platform. This type of collaborative, easy-to-do-business-with partnering is a signature of our team's operating model.

Through the use of the Akamai FastDNS service, single points of failure are inherently mitigated by the design of the solution. Our team will regularly evaluate this position throughout the life of the term so that the most cost-effective and technically sound solution is provided to the County.

Also included within our support activities is the maintenance of a comprehensive roadmap of all external DNS management services required in conjunction with Akamai and the County. This roadmap allows us to adequately inform our customer and plan time frames and completion dates for any software changes needed to improve service capabilities. As an integral part of these coordinated services, our SMEs will facilitate ongoing product and solution strategy planning with Akamai, so our collaborative roadmaps remain up to date with new and emerging functionality and service changes.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The LCM team proposes the continued use of the Akamai cloud-based resources as an integral part of our solution. We will operate and manage the service from our Rancho Bernardo site, where our support personnel will manage all aspects of the data network to include external DNS support services.

Our team leverages some remote resources, such as those from Akamai, and those support activities fall directly within the purview of one or more of our local SMEs for adherence to our customers' requirements, and we meet our service level requirements. During the new Contract, our team is proposing the same arrangement so that our SMEs and key personnel are able to maintain the collaborative interaction with the County that has delivered truly transformative results.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

An integral part of our continued support of external DNS services includes our integration with the County process, including the weekly network architecture meeting and the Enterprise Architecture Forum. As has been true for the past decade, our staff will participate in supporting continuous architecture and management activities for the internal and external DNS.

In conjunction with the County, HPES has refined our processes and methodologies for optimal customer support. From an external DNS perspective, our team works to establish new records or remove existing records based on the associated activation or deactivation of new services that tie to an external DNS service. Normally, this notification is received through the existing IMAR process.

- Automated Tools – Automated systems and tools involved in proposed solution

The LCM team uses the Akamai Luna Control Center accessed via a web browser to perform the essential activities of external DNS support. The Akamai and HPES teams use vendor-specific tools inherent in their offerings to support their services.

- Qualifications and Experience – Background and experience in comparable environments

On average our existing LCM team has more than 9 years of experience directly supporting the County as well as another 12 years of experience supporting customers who are similar to the County as a result of prior projects. Over the life of the existing Agreement, we have managed premise-based and cloud-based DNS services on various platforms, including the current solution.

In addition to the direct experience supporting the County, our staff leverages certifications that are directly applicable to the services we provide, including CCNA and CCNP.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

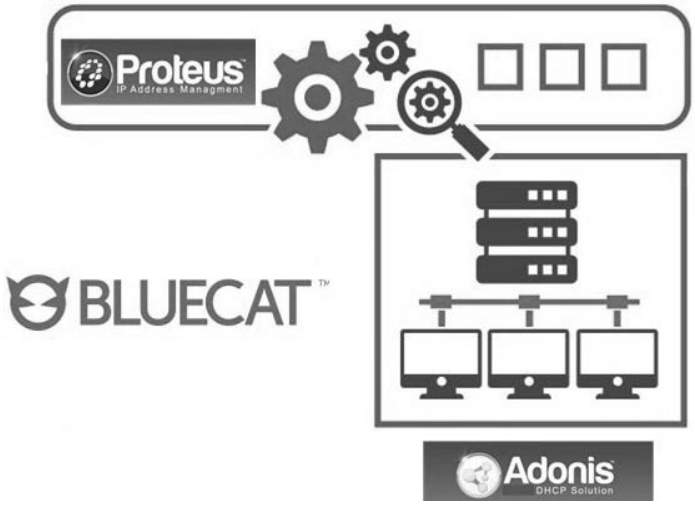
None.

IP Address Management Services (Sched. 4.3, Section 5.15)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Our comprehensive IP addressing solution is a fundamental part of our overall network support service and fulfills all of the requirements for IP Address Management (IPAM) services. Our solution starts with the BlueCat Proteus Enterprise IPAM v4.0.5-20 Platform as the single user interface providing integrated management of all static and dynamic addresses. Operating within the AT&T POP, this virtualized solution configures and documents changes to the IP address landscape and collects real-time information related to the current IP allocation within the network. A standby platform is presently located within the COC to mitigate against a single point of failure. In turn, the Proteus management platform communicates with the BlueCat Adonis appliances that are geo-redundantly located within the COC and the AT&T POP. These appliances serve as the policy recipients from Proteus and thereafter monitor, manage, and configure all Dynamic Host Configuration Protocol (DHCP) services within the County's internal network. The Adonis System also relays IP address utilization information back to Proteus for data aggregation, analysis, and presentation, as required. Our team proposes retaining this capability into the new Contract because it has proven to be a robust operational solution that can continue to provide return on investment. Figure 84 presents BlueCat's Proteus IP Management Solution.

Figure 84. BlueCat's Proteus IP Management Solution



BlueCat's Proteus IP Management Solution feeds the Adonis appliances with policy and configuration changes for distribution to the enterprise.

Due to the inherent capabilities of Proteus, our team uses this management platform for a structured approach to IP subnet assignment, to control static IP address use, and to monitor dynamic address allocation. Additionally, our solution allows IP address data to be collected, analyzed, and organized into the monthly DHCP pool and IP subnet utilization and trending reports for the County. In addition to providing automated discovery of IP addresses, this tool allows our engineers to detect and manage conflicting or duplicate address use quickly so that normal network operations are maintained.

At present, this solution set manages and controls the network domain using an IPv4 address schema, but it is fully capable of supporting IPv6 when address transformation is required. Presently, our teams support the equivalent of 916 Class C address blocks for internal, external, third-party, and public network access through our data networking services using efficient, fault-tolerant routing so that our services meet the County-specified service level requirements. Our solution is fully and continuously synchronized with the internal DNS services using the DHCP servers, which provide DHCP clients with the fully qualified domain name and IP addresses for DNS services. Additionally, Proteus provides Active Directory information regarding IP address assignments for System Center Configuration Management (SCCM). Via SCCM, efficient network utilization is maintained by designating Distribution Points (DP) within the domain to service adjacent blocks of IP addresses for system upgrades or patches. In this manner, blocks of IP addresses are automatically directed to the nearest DP, network traffic is localized to the extent possible, and latency is reduced.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The LCM solution continues to use the County Operations Center and AT&T POP for the reliability and resiliency IPAM services to help the continuity of network in accordance with service level requirements.

Additionally, our team will continue to use the AT&T Trade Street facility to house our local support personnel and manage all aspects of the data network, including IPAM. LCM plans the continued utilization of its local team, which has allowed close alignment with the needs of the County.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

An integral part of our ongoing IPAM services includes our SMEs acting as trusted advisors within the weekly network architecture meetings and the Enterprise Architecture Forum. Our SMEs will continue to use these venues to notify our user community of identified SPOFs or other enhancements and then implement our approved solutions. Additionally, our staff will also continue maintaining a comprehensive roadmap of all IPAM services hardware and software life cycles. This roadmap allows us to adequately inform and plan time frames and completion dates to stay within supported versions of hardware and software.

In conjunction with the County, we have refined our processes and methodologies for optimal customer support. From an IP addressing perspective, our support methodology focuses on four scenarios that require our staff's intervention to provide the County with timely service:

- **New Site Activation.** Our project management personnel are involved in the creation of any new site, and they include IPAM as part of the actively managed project plan. As needed, new block(s) of addresses are allocated for the site, and the recommended DP is also determined.
- **Site Decommissioning.** Again, our project managers are involved in any site decommission, and IPAM is part of the project plan as we recover existing block(s) of addresses for reuse.
- **Significant site growth projections.** Depending on the scale of growth projected, our project managers would be involved and include IPAM as a part of the project plan. In contrast, we use the IMAR process for smaller projects.
- **Static addresses are required.** To accommodate these requirements, we leverage the existing IMAR process to gain a static IP address, which is issued from a predetermined range for each site defined within the IPAM tool.

- Automated Tools – Automated systems and tools involved in proposed solution

Our SMEs use the BlueCat IPAM Adonis and Proteus systems to collectively fulfill all of the IPAM requirements and support our adherence to the service level requirements. Additionally, our staff also uses

CA Spectrum and eHealth to monitor the operational integrity of the enterprise and platforms so that risks are mitigated before they become operational issues.

- Qualifications and Experience – Background and experience in comparable environments

Our team will continue to use the experienced team that is now in place supporting the County to provide IPAM services. These staff members have numerous years of experience directly supporting not only the County, but also other customers similar to the County. In addition to our direct experience supporting the County, our staff leverages certifications that are directly applicable to the services that we provide, including CCNA and CCNP.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

New Site Installation Services (Sched. 4.3, Section 5.16)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

One of the key strategic initiatives for the County has been real estate planning and facility construction for the long term. This has resulted in the design and construction of new, state-of-the-art County sites. Since the beginning of the existing Agreement in 2006, the County has built 87 new locations throughout the region. The majority of these have been Leadership in Energy and Environment (LEED) certified; more than 30 have been awarded the highest level of LEED achievement. AT&T has partnered with the County and HPES to help plan, engineer, and build IT infrastructure in all of these locations through the new site installation services component of the Agreement.

The current structure of new site installation services categorizes new sites into tiers based on the number of network access, voice, or VoIP jacks resource units to be installed at each location. This has provided the County with the advantage of predictable telecom infrastructure costs when forecasting the overall financials for facility construction. It has had the disadvantage of restricting the County's flexibility in assigning structured cabling work to vendors other than the IT contractor when circumstances warrant.

To meet the County's requirement for the flexibility to engage its own cabling vendor, HPES has developed a solution that includes base services and optional services within the prescribed user based tiers that define the site types. This new RU structure will consist of 5 RU's by site type, with base and optional services within each.

Base services (the fixed component), will include activities such as pre-field work and requirements gathering, network design, circuit design/provisioning, installation of network hardware and project management that are required regardless of the cabling vendor used.

The optional services (the variable component), will include all cabling vendor activities as well as contractor project management oversight. These optional components are broken into two work categories to allow the County to select either all or a subset of the cabling work necessary at the new site. The first component within the optional services will be identified as "Riser Cabling". This component will include the placement of pathway and rack infrastructure as well as the placement and testing of fiber/copper based cabling runs between MPOE and MDF, and between MDF and IDF rooms/floors.

Trenching is not included in this service and will be the obligation of the County or their contractor to provide. The second optional component of the service will be identified as "Horizontal Cabling". Included in this service will be the placement and testing of all wall jacks, patch panels and plenum cabling between the IDF and the workstations or designated end points.

- Should the County elect to move one or both of these optional service components to a vendor of their choice, the resource unit will be decomposed to provide adequate cost recovery for the remaining New Site services. For example, in a situation where the County were to elect to do their own Horizontal and Riser cabling at a New Site, the cost of these activities would be deducted from the overall Resource Unit price and HPES would execute the base (fixed component) of New Site activities required to establish connection to the County network. Additional clarity on these fixed and optional services can be found in Volume III, Exhibit CC, 16.1-2.Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Resources we will utilize for this effort will include facility project managers and network design and field engineers. They will work out of the Trade Street AT&T facility. This team will conduct the design and planning function as well as the staging of all equipment used in the construction of the new site. They will also interface directly with County personnel at the proposed new site locations.

The proposed structure of the new site installation service will require involvement from the County's General Services organization in those cases where the decision is made to have the structured cabling and other components installed by the County's selected vendor. All new sites do require the County to provide certain components—such as power and air conditioning—that are determined on a project-by-project basis.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Our project management team uses standard Project Management Institute (PMI)-based Project Management Methodologies and has successfully used them to bring 87 new sites online for the County. These processes have been tailored to identify all site-specific activities needed to activate IT services at a new location. Our project managers (PMs) actively walk the proposed site with County stakeholders and engineering resources initially and at various points as the project requires. After requirements and the design are fully understood, the project plan, schedule, and task list are developed by project managers — laying out the details of the project as well as capturing internal and external dependencies. Identified as early as possible, dependencies under control of the County or County contractor are managed with a clear understanding of the associated impacts so that they do not become roadblocks to the project's successful completion. At project close, key learnings are identified and documented by the PM for sharing, learning, and continual improvement by the team.

Although external dependencies are not within our control, our team routinely focuses on these actions early in each project to mitigate the risk to completion of our deliverables. An example of this was the Health and Human Services Agency's move into their new Escondido facility. At a critical point in the project, difficulties in obtaining permits from the City of Escondido were identified. The AT&T team noted that these permits were a key dependency in the installation of telecommunications services to the site. To keep the project on schedule AT&T was able to leverage contacts within the City to obtain the necessary paperwork. Working in parallel, the AT&T PM also escalated internally so that AT&T leveraged resources were able to accommodate last-minute schedule changes and so that the County build and move-in schedule was maintained. For this effort, the product team was given the IT Customer Service Award by the County Technology Office.

Another aspect of our proposed processes include how project RU billing estimates and final billing are determined as follows:

- Project Start: The network design and pricing estimates documented in the initial Scope of Work will be based on the County-provided estimate of user occupants for the site.
- Project Completion: Upon project completion we will update the final user count in the SOW and present that to the County for project completion sign-off and billing initiation.
- Post Project 6 Months: We will perform a final true-up assessment 6 months from the County SOW sign-off. If the site user count has exceeded the tier limits for the new site RU originally billed then we will initiate a billing adjustment.

- Automated Tools – Automated systems and tools involved in proposed solution

Our solution proposes using standard project managements tools (such as MS Microsoft Project, Excel, and PowerPoint) in the planning and tracking of these projects.

- Qualifications and Experience – Background and experience in comparable environments

As the incumbent, HPES has supported the construction of 87 new sites over the term of the existing Agreement. The local project managers and engineers are experienced in the construction of new sites as small as two-person locations ranging to a size as large as the County Operations Center. They have an intimate knowledge of the technical components and processes required and have developed relationships with the key County stakeholders.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

An additional option that we recommend within the structure of this solution is to add a resource unit at the lower end of the site sizing table. It would be aimed at those locations that will hold between 1 and 10 County end users. Over the life of the existing term there have been more than 50 sites of this size constructed by the County. Including them in the proposed Type V Site (1–49 users) will present the County with a cost structure that might discourage the creation of these smaller sites. By carving this sized site out of the County-defined Type V category, these smaller locations will enjoy a lower-priced new site RU that is more closely tied to the costs required for their construction.

Previously communicated alternative approaches include a per "jack" based approach to optional (variable) services, where a more specific estimate of the cabling work (Riser or Horizontal) could be provided to the County. This option is not as predictable but could more accurately estimate the work needed for a given new site request within a site type range. Base services (the fixed component) apply in all cases and are necessary to conduct the work of building out a new site.

Interactive Voice Services (Schedule 4.3 Section 5.17)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Interactive Voice Services are defined as an IVS system which builds on the basic services provided in Voice Services, but includes one or more of the following capabilities:

- Call Management Reporting
- Call Recording
- Speech Recognition Application

- County data integration (data dip)
- Wallboard (Physical/Virtual)
- Computer-Telephony Interface (screen pop)
- Work Force Optimization
- Outbound/Predictive Dialer
- Agent Softphone
- Speech Enabled Customer Surveys

Three categories of IVS will be created. Each will provide for technical design, infrastructure, licensing, hardware/software maintenance and support and initial user training. The categories will contain the following components:

- **Small IVS** – *includes Automated Call Distribution (ACD) and/or Auto Attendant (AA) & Call Management System*
    - Automated Call Distribution (ACD)
        - Distributes calls to customer facing agents.
        - Supports the total contact center agent population at all County network locations.
        - Includes trunking infrastructure to support the routing of calls.
        - Can be used as a stand-alone component or in conjunction with an Auto Attendant.
    - Auto Attendant (AA)
        - Supports Touch-tone input to route calls across the County voice network.
        - Includes the professional recordings both English and Spanish menus and prompts.
        - Includes trunking infrastructure to support the routing of calls
        - Can be used as a stand-alone component or in conjunction with an ACD.
    - Call Management System (CMS)
        - Provides reports of contact center agent metrics such as abandoned calls, average talk time etc.
        - Used in conjunction with an ACD to manage contact center performance.
        - CMS is the additive feature which initiates the Small IVS RU category vs. the right-to-use ACD and/or AA capability associated with the Voice RU's.
- **Medium IVS** – *includes all components from the Small IVS RU category and will also include:*
    - Automated Call Recording (ACR)
        - Provides for up to 90 days of customer agent recorded calls for both compliance and quality purposes.
    - Virtual Wallboards
        - Provides ACD statistics and messages displayed on contact center agent and supervisor desktops.
    - Agent Softphone

- Provides IP softphone via a desktop client that will provide County contact center agents full functionality whether they are working at their primary County facility, a remote/alternate County site or at home.

- **Large IVS** – *includes all components from the Small and Medium IVS RU categories and will also include:*
  - Interactive Voice Response (IVR)
    - Platform for custom applications such as outbound predictive dialing, multi-language support, voice recognition and County data integration.
  - Computer-Telephony Interface
    - Customizable interface between IVR and Desktop components to provide database information to a contact center agent when a constituent calls.
  - Short Message Service (SMS)
    - Provides up to 200,000 outbound text messages to specifically defined County client lists.
    - Requires the manual upload of a County file of customer contact information to the hosted platform.
  - Work Force Management
    - Centralized platform of work force scheduling, forecasting and adherence of contact center agents.
    - Provides long term strategic forecasting of agent resource requirements based on historical data
    - Integrated with CMS for agent call statistics
  - Physical Wallboards
    - Provides ACD statistics and messages displayed on physical monitors in County call centers
    - Includes the controller infrastructure and supporting software to County provided monitors

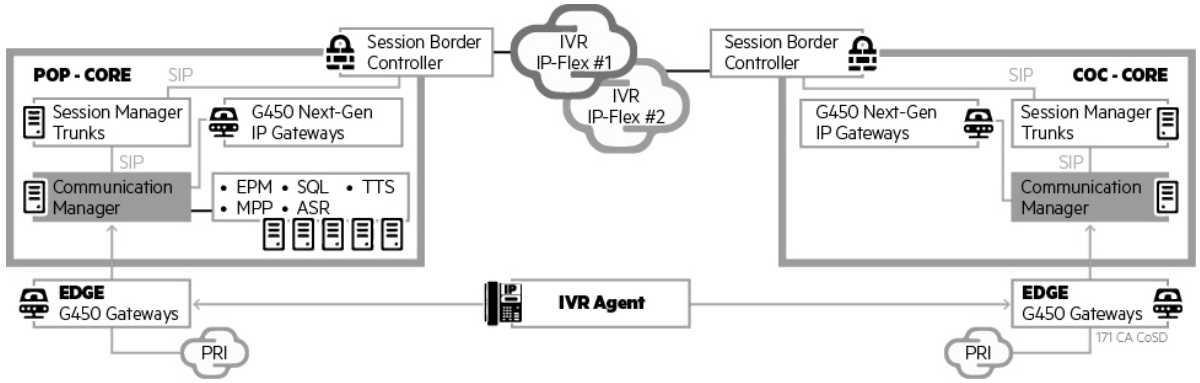
Integrated Voice Response

At the core of the functionality provided under IVS Services is the Integrated Voice Response platform. The County's IVR infrastructure is built around the Avaya Experience Portal, located at the AT&T POP. This platform provides IVR, self-service, touch-tone as well as speech recognition services for key contact center solutions across the County such as the Department of Animal Services, the Land Use Environmental Group, and various departments within the Health Human Services Agency. This scalable, high-availability infrastructure provides many options for programming and agent integration—allowing customization for any type of constituent-facing contact center service.

The platform will undergo near-term changes relative to external telephony connectivity as AT&T initiates plans to implement dedicated, fault-tolerant inbound and outbound IP Flex SIP trunks for the County's IVR infrastructure at the AT&T POP and County Operation Center. This IVR solution will not impact enterprise voice traffic, allowing business units to conduct high-volume contact center activities, such as outbound dialing campaigns. This new capability will allow for a more standardized resource unit base from which business units can leverage the platform. This upgrade is proposed as an initial transformation initiative and included in Voice Services as a means to meet relevant scope requirements. Further details of AT&T planned transformation of IVR services is defined in Section 2.12, Transformation Services, subsection "Initiatives: Voice Services Transformation."

Over the term of the Agreement, AT&T will develop a transformative roadmap, where proposals will be developed to increase the redundancy and resiliency of IVR applications, as well as to provide additional feature benefits, such as automated agent call-back and web chat. Figure 85 presents Avaya's Experience Portal connectivity.

Figure 85. Avaya's Experience Portal Connectivity



Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The County Operations Center and AT&T POP will be the primary facility locations for IVS services. Over the life of the term, HPES will work to implement geo redundant systems for key functionality as well as make proposals to introduce new features and functionality. Refresh will be performed for the systems on a five year basis.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

As mentioned above, the process for changes and enhancements needs reflect the County's need for flexibility. For minor/basic changes to existing voice applications, we propose that the County may make these types of changes at no additional cost.

- Additions, changes or deletions to existing call flow/menu prompts
- Additions, changes or deletions to existing routing or transfer points
- Implementation of licenses associated with provided features
- Professional voice recording of changes on basic Auto Attendant and ACD systems

For more custom changes or enhancements (a recent example includes the new "zip code routing feature" for the Healthy San Diego IVR which involved County data integration and custom application design) the County will use the Work Request process to order the features. This will allow the County to use the one-time money when it is available for this work – this is a common request.

As new technologies or capabilities become available, they will be evaluated by the Network team on a case by case basis. Implementation of these features could either be amended to these RU's or created as a separate RU dependent on their scope and complexity.

- Automated Tools – Automated systems and tools involved in proposed solution

Call Management System: Provides reports of contact center agent metrics such as abandoned calls, average talk time etc.

Automated Call Recording: Provides for up to 90 days of customer agent recorded calls for both compliance and quality purposes.

Workforce Management System: Centralized platform of work force scheduling, forecasting and adherence of contact center agents.

- Qualifications and Experience – Background and experience in comparable environments

HPES has provided all IVS services for the County of San Diego for the last 10 years. Over this time, new features and functionality have been developed and implemented such as the Experience Portal IVR, Workforce Management, SMS capabilities and more. Our team continues to move with the industry to ensure training of resources as new functionality and solutions are brought to the County.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

2.8.1 Offeror Response to Network Services Specific Questions

2.8.1. Describe your proposed approach to bandwidth and capacity management and reporting.

As the incumbent provider, HPES has tailored its bandwidth and capacity management processes to meet the County's increasing needs. These processes have evolved over the life of the existing Contract and have now reached a level of maturity.

Bandwidth is proactively delivered to County locations before links saturation affects performance. This process begins with weekly reporting on key capacity metrics using our CA spectrum and eHealth tools. These tools trend bandwidth and latency against baselines. These trends are validated as legitimate business traffic using our deep packet analysis tools (see Sections 2.8.2 and 2.8.6 for more detail) before action is taken.

Using mutually agreed thresholds, our Capacity and Performance Monitoring team will make recommendations for bandwidth upgrade in the weekly Operations Governance. This approach to capacity management helps the County of San Diego provide the right level of capacity at the right location and at the right time.

Below are the proposed thresholds for both WAN and Internet Transport:

Bandwidth Utilization Threshold (WAN): 90% Peak Utilization over 4 week period of time + corresponding latency threshold breach

Bandwidth Utilization Threshold (ISP): 90% Peak Utilization over 4 week period of time + a 1.5 – 2Mbps drop rate

Latency (WAN): GigaMAN (greater than 4ms), Opt-E-MAN/NoD (greater than 8 ms), T1 (greater than 15 ms)

As part of this process, the Contractor provides:

- Weekly review of network capacity metrics as part of the County's operational governance process.
- Capacity management that meets the business needs of the County using tools that provide real-time threshold alarming.
- Communication of findings and recommendations that help the County achieve optimal utilization and capacity.

The local team will continue to meet weekly with the County's operational team to present and review findings and make recommendations. We will perform optimization analysis daily using our automated tools that aggregate findings and establish trends that become the basis of our weekly reporting.

As we move into the new Contract, network transformation will migrate remote sites to AT&T's Switched Ethernet (ASE) with Network on Demand. This allows the bandwidth and capacity management practices for the County to become even more dynamic. Using the software-defined networking capabilities that are inherent to ASE with/Network on Demand, bandwidth can be adjusted from as low as 2 Mbps to as high as 1 Gbps in 15 minutes.

In the near future, adjustments can be made within the Network on Demand infrastructure on a scheduled basis, providing the County a great deal of flexibility in bandwidth management. As an example, if the County Health and Human Services Agency planned an employee training event that required heavy video and interactive content (not distributed using a centralized, multicast town hall solution), our capacity team will schedule an adjustment to specified remote sites for an agreed period of time. This would deliver the required bandwidth where needed and, at the completion of the training, automatically adjust the bandwidth back to its normal business capacity.

Real-time bandwidth adjustments can also be made as needed. This may be required as the result of unexpected local or national events creating unanticipated demand on the data network. One example occurred in May of 2014, when wildfires flared up in North San Diego County. Many of the County employees looked to streaming news content to understand the implications for County business as well as for family and friends. This event created an unforeseen need for Internet bandwidth, which we were quickly able to react to by dynamically adjusting the ISP bandwidth to allow the traffic to burst above the normal Committed Information Rate (CIR). As future events occur, our team will be able to do more than just increase the ISP bandwidth. By using our capacity and performance monitoring tools, we can analyze the traffic and determine if it is affecting the County's WAN. At that point, real-time adjustment can be made to alleviate the congestion in minutes, something that previously would take days or even a week to execute.

All transport services—including WAN, AVPN/MPLS, ISP, and SIP trunking—can be scaled to maximum interface capacity as well as built in parallel so that growing County bandwidth needs are met over the life of the term. Also, as new services are made available with additional speed or throughput capabilities, AT&T will evaluate the feasibility of such services and make corresponding upgrades where reasonable under existing service commitments.

Our approach to capacity and bandwidth management has evolved during the past decade by creating the tools and information that has provided County users the network capability to do their daily jobs.

Additional capabilities in the new term will make these processes even more efficient and better able to meet the future needs of the user community.

2.8.2. Describe your proposed approach for performance monitoring and reporting, and how it will affect bandwidth provisioning.

HPES' existing performance monitoring and reporting capability provides the data necessary to optimize network service to the County. Capacity planning is used to determine the network resources necessary to prevent performance issues from impacting these critical network services. Performance monitoring/management is the process of managing network and data services response times, consistency, and overall service quality.

HPES' network team currently administers, monitors, maintains, and manages performance of the data network services and network services infrastructure. This involves input from many areas of the business to identify what IT infrastructure is required to support the County's business.

The process components include:

- Performance monitoring for routers, switches, firewalls, and network servers and appliances
- Capacity monitoring of WAN transport circuits
- Internet performance monitoring of public and staff CIR
- Trend reporting and analysis.

Key sub-processes are:

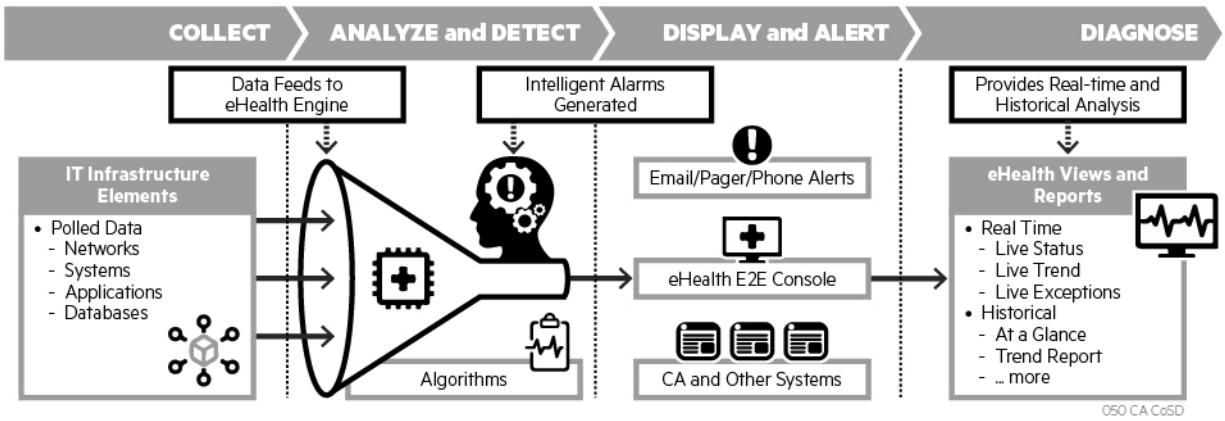
- Network bandwidth monitoring to specified thresholds
- CPU/memory utilization and errors monitoring on all network devices to specified thresholds
- Responsive impact assessment and mitigation planning
- Proactive trend-based "situational watch list" assessments and corresponding action plans
- Real-time traffic analysis initiated from "exceeded threshold criteria" in the form of Spectrum critical alarms.

Performance Monitoring Tools

AT&T's capacity and performance management functions utilize various toolsets that provide monitoring, reporting, trending, and analysis services to the County network team.

CA's eHealth and Spectrum tools integrate to maintain critical service levels across complex network environments by combining eHealth's automated availability and performance management with the Spectrum network service and analysis platform, as shown in Figure 86.

Figure 86. Automated Availability and Performance Management



The eHealth data collection process collects, analyzes, and alarms against performance thresholds.

The eHealth and Spectrum tools allow for more efficient alarming and reporting, enabling the network capacity and performance management team to focus on proactive troubleshooting, performance optimization, and service level management.

Another toolset that helps manage system performance within the County network infrastructure is Riverbed Cascade Profiler, which provides a unified end-to-end view of service delivery, application, and consumption from the data center to the end user. Cascade Profiler assists in troubleshooting the threshold deviations reported in eHealth, troubleshooting in real-time and from a single probe interface. Cascade retrieves real-time information, providing quick and easy access to logical views such as link analysis, link usage over time, Top N applications, and Top N conversations and hosts.

Troubleshooting and Forensics

The above mentioned promiscuous tools enable event correlation and forensics through the active capture of network traffic combined with reporting capabilities that provide real time and historical data. This capability applies not only to the previously mentioned tools, but also includes the deployment of desktop based tools such as Wireshark, which are used as needed to conduct packet captures from individual assets. When used in active troubleshooting, all of these tools are used to correlate the event to a root cause for resolution by the appropriate framework using cross framework troubleshooting processes.

Performance Baselines

Our tools provide data on specific metrics for historical and baseline performance evaluation. These baselines are important in our monitoring of the County's network since they can directly affect bandwidth provisioning and other resources. The following is a sample of some baseline data collection components that AT&T uses in performance evaluation.

- **Automated Baseline Data Collection**. eHealth uses upper limits for use and errors— referred to as trend thresholds—to identify problem areas. Thresholds are collected and sorted into "health indicators" for Situations-to-Watch Reports.
- **Remote Site Latency Baseline**. One of the most important tools used to manage network performance is the latency baseline for each network node. Latency is determined by the round trip response time from the polling server/system (located in the AT&T POP) to the remote site router and back to the Server. These statistics are collected every 5 minutes. Sites that deviate significantly from the rolling average in a given week are investigated further with deep dive analysis to determine if a persistent

issue is occurring or if the event is considered a one-time anomaly. Weekly data is also compared the previous week's results to determine a trending pattern.

- **Network Security and Systems Device Baseline**. eHealth monitors all systems and server variables (CPU utilization, memory, disk space) using simple network management protocol (SNMP) polling and follows the capacity and performance threshold metrics. The systems that are monitored include all managed firewalls, intrusion detection and prevention (IDPs), radius, proxy, Dynamic Host Configuration Protocol (DHCP), DNS, and VMWare servers.

Performance Threshold Alarming

Once baselines have been determined, thresholds are then established based on variables within the network infrastructure. Circuit measurements depend on bandwidth to determine baselines and thresholds. Physical devices such as routers and switches report memory allocation errors, CPU utilization, and buffer hits. There are also broader ranges of environmental specifications to which thresholds are tracked, such as power supply, fans, and temperature, among others.

The County's threshold values currently include the above parameters formulated by collected baseline data as well as vendor recommendations and industry standards. Exceeded thresholds can be and have been alleviated with bandwidth increases, IOS upgrades, hardware refresh, and topology redesigns as well as through application or system level adjustments.

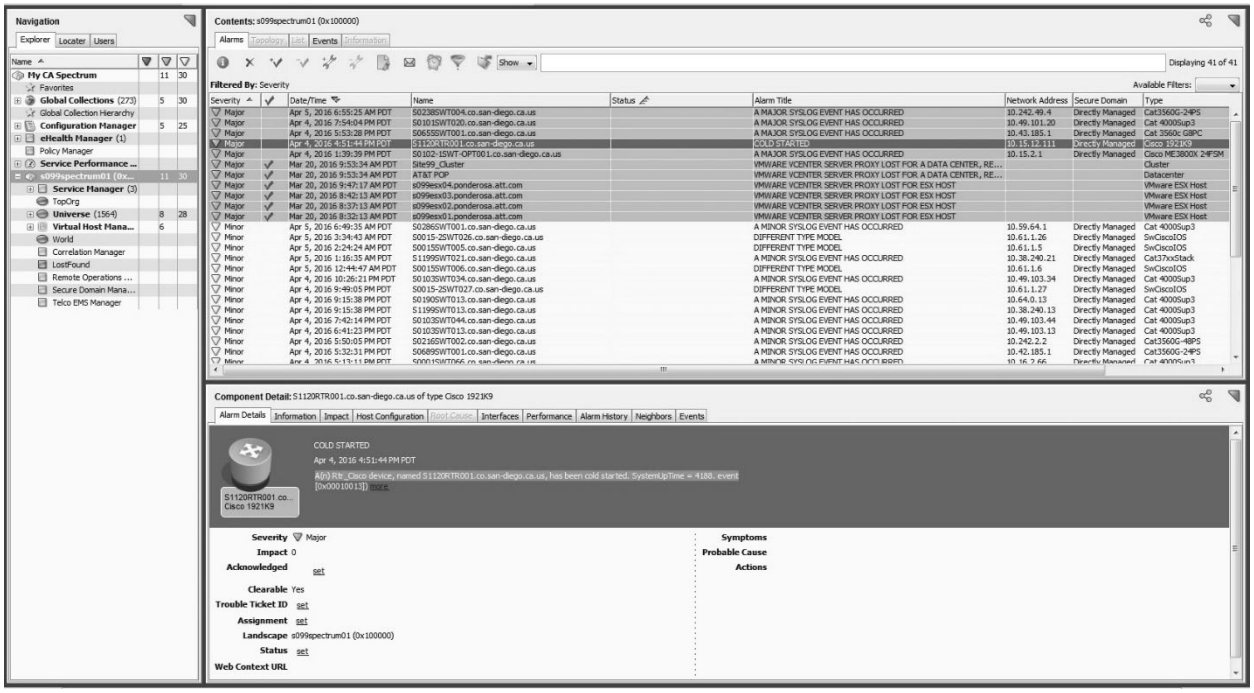
Threshold severity is currently defined in four levels, each dictating an appropriate course of action as listed in Table 53.

Table 53. Threshold Severity

SEVERITY	ACTION
Warning	Track element status on weekly basis.
Minor	Add to Watch List (document in Situation-to-Watch and status any changes).
Major	Assess and engage relevant framework, open internal ticket if necessary. Add to Watch List.
Critical	Trigger to "Attention" notification tool, initiate internal break-fix. Troubleshoot and actively mitigate until resolution.

Critical alarms are sent to the Attention application system that notifies the NOC operations team (and on-call) members via phone, SMS, and email. The Attention system software provides a predefined notification process for critical alarms as well as escalation processes for overdue or pending alarms on a 24x7 basis as demonstrated in Figure 87.

Figure 87. Alarm Thresholds Notification Function



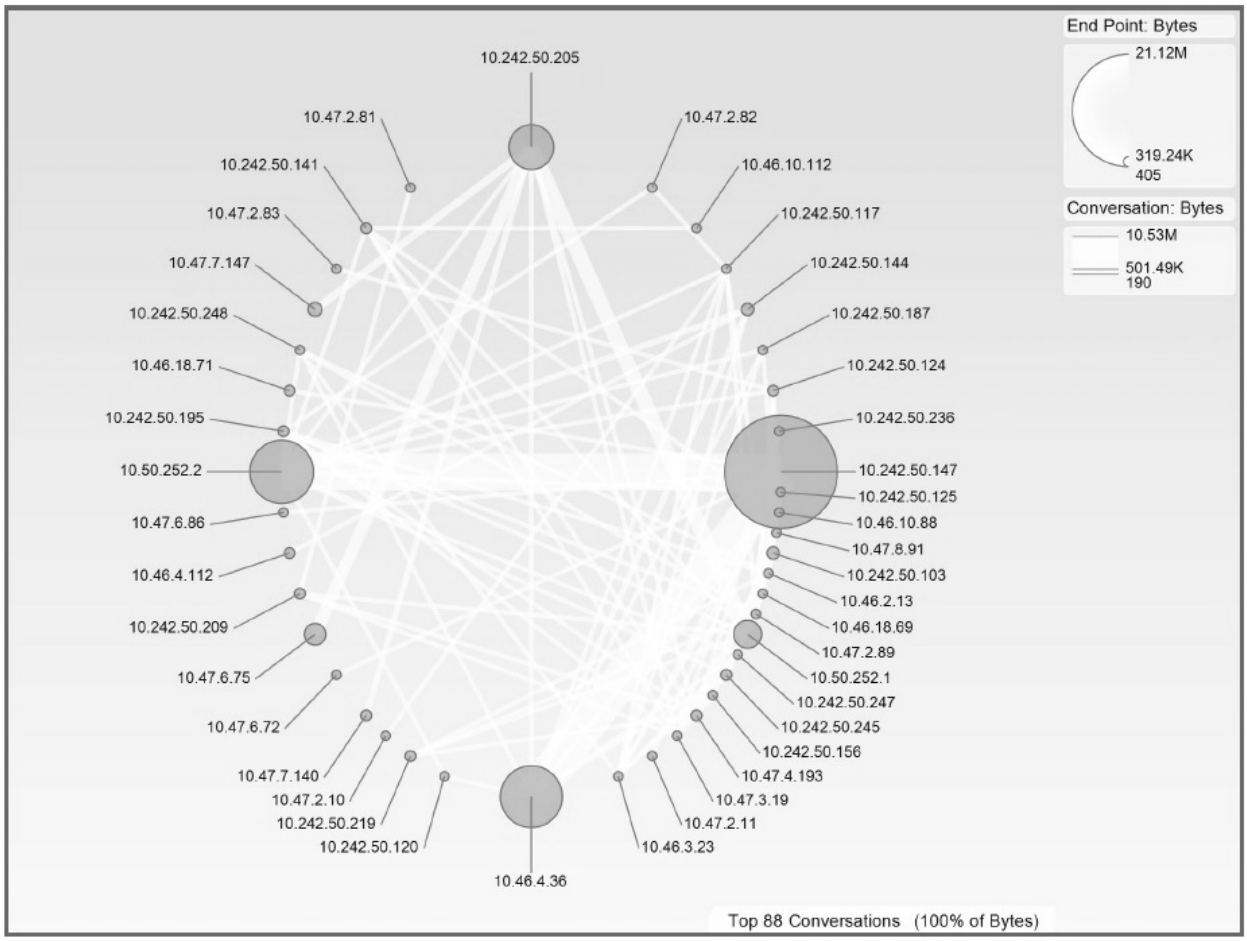
CA Spectrum's Threshold Alarming function provides real-time view into various alarm categories, with the ability to drill down on each event.

Other important thresholds that have been established include site latency and Internet CIR thresholds. Site latency thresholds include latency deviation based on the type of circuit. Internet CIR thresholds are triggered when bandwidth use on the Internet link goes 20% above the daily average, as measured by eHealth and in conjunction with quality of service (QoS) policies applied to the Internet router.

Performance Trending and Analysis

Once baselines and thresholds have been established, trending and analysis takes place. There are a number of variables that contribute to the analysis of a trending element. Bandwidth use, CPU use, physical hardware errors and application response time delays can all have an impact on network health. eHealth reporting (Situations-to-Watch, Top N Reports defining baseline statistics, Health Index Reports indicating CPU, errors, and discards) along with Cascade Profiler reporting (application response time statistics, link usage, top application layer applications and hosts) can collectively qualify and pinpoint performance degradation associated with the network or an application. This detailed information, as depicted in Figure 88, drives necessary corrective actions as well as engagement of the appropriate HPES framework in problem resolution.

Figure 88. Trends in Traffic Patters across the Network

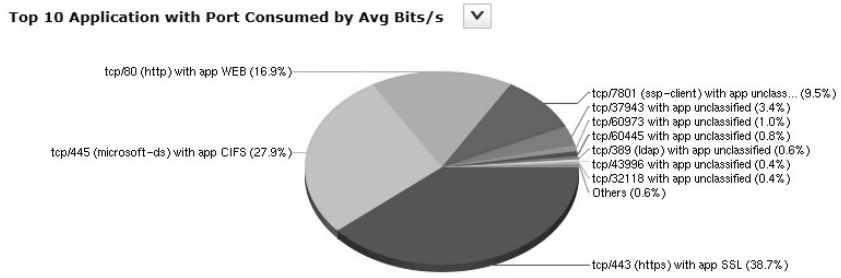


The Riverbed Cascade tool is able to identify traffic patterns across the enterprise, allowing for drill down on specific network segments.

Reports showing an increase in trending for elements in the network are reviewed and investigated for further analysis. Report trending from Situations-to-Watch, Top N latency, and health index reports are addressed by further analysis with a deeper dive into the affected element(s).

Adjustments made to correct issues associated with variables related to bandwidth use, memory allocation errors, CPU processors, or other changes in the network, are based on investigation of the specific cause. Increasing the bandwidth for a specific County site is determined by identifying historical data and trending analysis for a specified period of time. There is an initial assessment and continued monitoring of the network thresholds (Figure 89) (application, user count, throughput and other associated activities) to validate the appropriate remedy for a given issue.

Figure 89. Riverbed Cascade Tools



Application with Port Consumed 1 - 20 of 44

Port-Application	Avg Bits/s ↓		Avg Packets/s		Avg Active Connections/s		Avg Net RTT (ms)	Avg Server Delay (ms)	Avg App Bits/s per Conn	Avg Conn Duration
tcp/443 (https) with app SSL	626,287	(39%)	130.85	(42%)	1.09	(34%)	32	91	13,336	20 minutes 50 seconds
tcp/445 (microsoft-ds) with app CIFS	451,476	(28%)	77.60	(25%)	< 1	(3%)	43	1	80,904	6 minutes
tcp/80 (http) with app WEB	273,695	(17%)	48.48	(16%)	< 1	(19%)	39	60	154,568	1 minute 42 seconds
tcp/7801 (ssp-client) with app unclassified	153,959	(10%)	23.03	(7%)	< 1	(14%)			42,128	15 minutes 59 seconds
tcp/37943 with app unclassified	54,318	(3%)	13.89	(5%)	< 1	(3%)			184,680	2 hours 13 minutes
tcp/60973 with app unclassified	16,091	(< 1%)	3.56	(1%)	< 1	(2%)	3		40,808	59 minutes 3 seconds
tcp/60445 with app unclassified	13,021	(< 1%)	2.36	(< 1%)	< 1	(1%)			1,896	3 days 18 hours
tcp/389 (ldap) with app unclassified	9,116	(< 1%)	2.19	(< 1%)	< 1	(1%)			-	1 second
tcp/43996 with app unclassified	6,492	(< 1%)	1.58	(< 1%)	< 1	(1%)	< 1		38,480	41 minutes 42 seconds
tcp/32118 with app unclassified	6,226	(< 1%)	1.16	(< 1%)	< 1	(< 1%)			15,056	
tcp/8003 with app unclassified	3,013	(< 1%)	1.04	(< 1%)	< 1	(< 1%)	17	64	1,416	38 seconds
tcp/82 (xfer) with app unclassified	2,319	(< 1%)	< 1	(< 1%)	< 0.01	(< 1%)	48	1,979	68,624	2 minutes 15 seconds
tcp/88 (kerberos) with app unclassified	1,340	(< 1%)	< 1	(< 1%)	< 1	(1%)			-	110 ms
tcp/9080 (glrpc) with app unclassified	914.74	(< 1%)	< 1	(< 1%)	< 0.01	(< 1%)	41	203	72,688	10 seconds
tcp/49158 with app unclassified	422.12	(< 1%)	< 1	(< 1%)	< 1	(< 1%)			-	33 seconds
tcp/49155 with app unclassified	216.96	(< 1%)	< 1	(< 1%)	< 0.01	(< 1%)			-	31 seconds
tcp/135 (epmap) with app unclassified	210.22	(< 1%)	< 1	(< 1%)	< 1	(< 1%)	50		768.00	21 seconds
udp/53 (domain) with app unclassified	204.68	(< 1%)	< 1	(< 1%)	< 1	(6%)			-	
udp/389 (ldap) with app unclassified	63.44	(< 0.01%)	< 1	(< 1%)	< 1	(< 1%)			-	
tcp/8082 (us-cli) with app unclassified	49.69	(< 0.01%)	< 1	(< 1%)	< 0.01	(< 1%)	< 1	40	20,880	179 ms
Others	350.68	(< 1%)	< 1	(< 1%)	< 1	(11%)				
Total	1,619,786	(100%)	308.23	(100%)	3.17	(100%)				

1 2 3 go to page 1

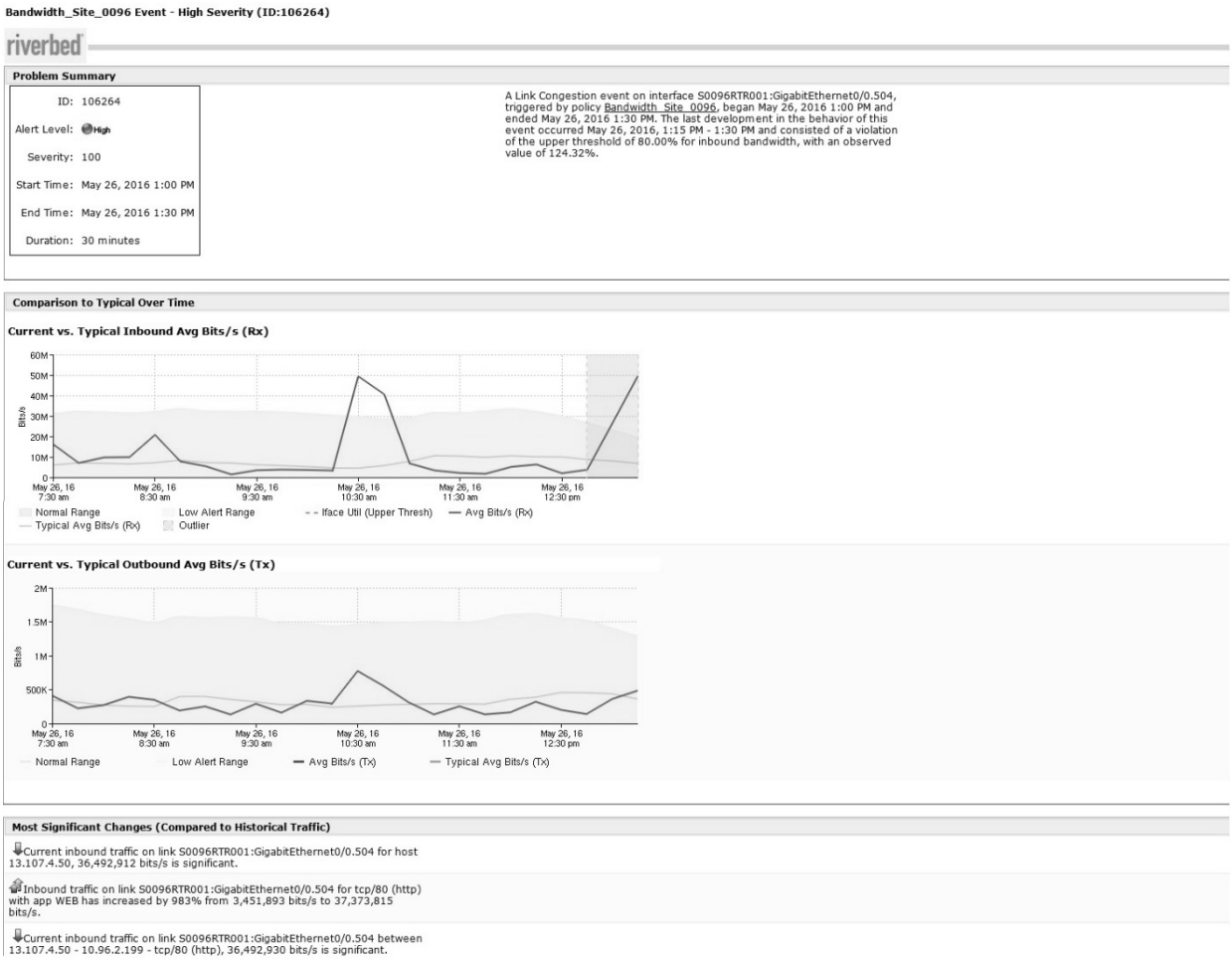
The Riverbed Cascade tool's deep packet analysis capability provides specific application level detail, used in forensic and real-time anomaly detection.

Whether it is a bandwidth increase due to consistent high utilization trends, identifying a hardware, software, or application-based resolution, or even a necessary change in network topology, adjustments are made appropriately to resolve the issue(s) surrounding the trend indicators.

Real-Time Anomaly Detection

As the HPES Operations team begins developing processes around real-time anomaly detection, they will develop automated alarming and event correlation capabilities, with focus on application performance. The tools mentioned in this section—along with other data center and desktop-based platforms—will enable a layered approach to event triangulation, which, combined with the daily stand-ups highlighted in Section 2.8.6, will improve the proactive performance management of services across the enterprise. Currently, the Riverbed Cascade tool is being tuned in a collaborative, cross-framework effort that is already yielding results that are helping establish new monitoring elements, baselines, and thresholds. This is an area that the HPES team will dedicate resources to improving proactivity over the life of the term, with measured results reported through the operations governance process.

Figure 90. Riverbed Real-Time Anomaly Notification Example



The Riverbed Cascade tool's deep packet analysis capability provides specific application-level detail, used in forensic and real-time anomaly detection.

Our team continues to tune the tools like Riverbed Cascade to enable real-time anomaly detection. These automated reports can be used in conjunction with other tools to correlate events and resolve issues in a proactive manner.

Data Aggregation and Analytics

Our team will contribute key capacity and performance tool data to the cross functional data warehouse, with focus on bringing enabling automation and continuous improvement through a global analytics and reporting practice.

We are committed to continuous improvement and, over time, we will work with the County in extending both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured in terms of a number of ways, such as:

- Service Strategy and Improvement Analytics: This area focuses on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis
- Service Design Analytics: We see this as a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data we can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.
- Service Operations Analytics: Blending ITSM data and benchmark IT performance data, we can conduct analysis to reduce business impact of events, incidents, and problems.
- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

Performance Reporting
With the appropriate tools already in place, baselines and thresholds completed, and trending and analysis processes established, AT&T currently provides a number of reports to the County that affect not only bandwidth provisioning, but adjustment and potential corrective action to a wide variety of County resources. On-demand reporting is available for fast turnaround on critical and time sensitive issues.

Trend and health reports are scheduled monthly to collect data and identify the top volume and health index leaders throughout the County network infrastructure. The report identifies contributors that qualify for threshold conditions such as, use, CPU, memory, errors and latency.

Elements each month are sorted by the Top N elements and performance indicators that require attention or resolution. A summary analysis is presented for the monthly activity and provides watchful situations or those exceeding threshold limits that require corrective actions.

Included in the monthly reports is a "Monthly Summarization Report." The details in this document include opened tickets for County sites that were affected by latency, bandwidth, errors, CPU, and memory related performance issues.

AT&T has the tools, personnel, processes, and reporting in place to continue providing the County with a network that not only meets today's needs, but continues to transform with the flexibility to meet future needs and services provided to the community.

As we look forward, new and layered approaches to integrating capacity and performance and real-time anomaly detection are being defined that will leverage multiple toolsets. This will involve cross-framework teams that proactively respond to enterprise issues affecting end users. These new approaches are discussed in Section 2.8.6 of the Framework Specific Questions.

2.8.3. Describe your proposed strategy to identify and eliminate single point failures in Network Services.

As a defining body in the region, the County provides critical services to its constituents, which if interrupted can have devastating effects on the safety and stability of the community. Further, the County has defined itself as a leader among its peers, using technology in every aspect of its public services. From providing better child welfare services to using mobile devices for employees that allow real-time retrieval of case information to the transformation of the library system to providing public Internet at no charge to members of the community, the County increasingly relies on the continuity of the data network for its business functions to remain operational under any circumstance. With this in mind, HPES has focused heavily on redundancy and survivability of critical core network services during the life of the existing contract.

In an accelerated pace during the last 3 years of the existing contract, HPES has transformed the network core, building out a second point of presence at the County Operations Center. This site was chosen for its central location and inherent facilities redundancy that includes backup power capability and diverse telecommunications entrance facilities. This second network point of presence provides active and dynamically available services such as data center connectivity, wireless controllers, voice call control, Internet access, session initiation protocol (SIP) telephony trunks, IDS/IPS, firewall, SSL VPN, MDM gateways, domain controllers, print servers, and network systems infrastructure such as our performance monitoring and alarming solution.

This new geo-redundant network core has established a foundation for future initiatives where the ongoing and focused effort to eliminate single points of failure are now incorporated into all aspects of service delivery. Looking forward, our transformation initiatives will leverage this design as we move towards cloud services enablement and the elimination of legacy technology (such as T1s, Centrex voice services, and PRI's) from the network.

In the broader carrier network, we avoid single points of failure in our network elements (such as circuits, central offices, and core network elements) via its redundant network design and software defined infrastructure. These redundancy solutions allow AT&T to maintain continuity of the regional, nationwide, and global backbone in the event of isolated failure. One dynamic of the County network solution leverages this redundancy through the use of diverse pathway and ISP exchanges in both San Diego and Gardena, California. With this configuration, the geo-redundant County ISP service will remain dynamically available in the event of a regional service interruption.

This relentless focus on business continuity demonstrates a real and tangible alignment of vision between the County and HPES. As members of our community, and indirect servants of the public good, we recognize our obligation and our ability to help support the continuity of Government.

2.8.4. Describe your proposed approach to network persistence and application persistence in Remote Access Services.

In support of the County's vision of a "Government without walls," HPES has implemented a remote access solution that leverages redundant infrastructure with software enabled network and application persistence. This multiplatform solution was designed and delivered to meet specific business purposes, starting with the functionality of SSL VPN and then expanded to provide application persistence for mobile users that actively interact with enterprise data while physically in motion and in turn are exposed to the connectivity interruptions that can occur across carrier mobility networks.

In 2015, network persistence was enabled through a software upgrade on the Pulse Secure SSL VPN service. This capability makes sure that minor connectivity interruptions in network connection do not affect the VPN session, which provides a layer of protection for most users on a managed laptop while operating outside of a County facility in a static position.

As remote access technologies continue to evolve, HPES will seek to consolidate the network and application persistent capabilities that are currently being provided on two disparate platforms. Our approach will evaluate options for consolidation of the remote access architecture and/or services.

This objective will take into account the current investment cycles cost to the County, as well as the appropriate geo-redundancy of the solution design and performance. User experience, impact to business associated with a change in solutions, as well as providing the proper levels of support will be carefully weighed for any and all solutions under consideration.

Our approach is to take a transformative approach to this goal, evaluating the best options for the County in the term of the agreement. We will continue to closely monitor industry trends, vendor roadmaps, and

innovation in the remote access space to properly evaluate and select the best solution for the County. We will work closely with vendors to determine the optimal solution in terms of reliability, usability, functionality, features, and the ability to make full use of the redundant network architecture to preclude any single points of failure as part of the solution.

2.8.5. Describe your proposed approach to Voice Services with respect to VOIP (e.g. do you recommend a different or more aggressive approach than prescribed in Schedule 4.3?).

HPES has deployed more than 6,000 VoIP endpoints at nearly 20 County sites during the past 5 years. While the TDM/digital voice environment has remained stable and functional over the term of the existing contract, the migration of the remaining 80 PBX/TDM sites is now poised for transformation. In anticipation of this event, the HPES team has upgraded the Avaya and Cisco infrastructure such that the migration of the remaining end points to an Avaya VoIP solution can be done at relatively low cost as compared to a wholesale migration to an alternate call control platform. SIP Trunking is being expanded to include LD and Toll Free 800 calling to substantially reduce, and in some cases eliminate, usage charges.

HPES believes that the transformation plan outlined in our response to Schedule 4.3 in Exhibit KK, Section 3.5, takes advantage of the resources the County has already invested in the current VoIP solution while keeping options open to analyze other alternatives as they become available and are evaluated over the term of the agreement. Other options could include migration to new call control solutions or even a shift to cloud-based voice services. It is critical that the County not be boxed-in to a technological corner as voice and unified communication capabilities converge. With this approach, we will continue to move the existing infrastructure forward in a cost effective manner while adding features and functional benefits to the County's end users.

2.8.6. Describe your proposed approach to increase visibility into all data communications and data flows between End-Users and Services within the Data Center.

HPES manages a wide range of platforms that provide unique sets of detailed information available in both report and real-time format. It is a complex and big challenge to address chronic issues in the environment—by the time they are well understood, they have generated customer dissatisfaction and wasted troubleshooting efforts. This leaves the operations team with the challenge of working through the symptoms and contributing causes to determine the root cause of the issue. The fact is, it takes the same tools and effort to troubleshoot these issues after they have become significant problems as it does to address them proactively.

Effective tools are not the problem facing proactive performance management. It is the practice of modeling, trending and analysis that can unlock the potential of the data the tools can deliver, if performed with a broad understanding of the enterprise.

The approach that HPES believes best to attack this situation is to create a cross-framework, predictive analytics team whose charter is to manage performance on an enterprise basis. This team will execute a repeatable process using a layered approach using numerous tools to monitor and respond to shifts in baseline data.

By developing baseline traffic patterns for network, application, desktop, server, and management traffic, this team will define thresholds and event patterns, allowing the team to take predictive action, correlating anomalies in the environment. Using the multiple sources of data, HPES will conduct daily stand-up calls where threshold breaches will be evaluated and diagnosed. This team will open internal operational tickets on the issues and will have the authority to escalate across any framework to engage resources as needed to respond and identify the source of the anomaly. Ongoing reports will be provided to the County

operations team and covered in weekly governance meetings, identifying open issues that are being monitored as well as successful closures.

HPES' County Operation team will also be tasked on an ongoing basis with improving processes, tuning their practices to better predict, correlate and resolve anomalies. This team will also have the responsibility to train on their tool sets, improving their mastery in the art of performance analytics. Further, HPES will evaluate new and emerging tools that will proposed for implementation, adding to the depth of the data sources at the County's disposal.

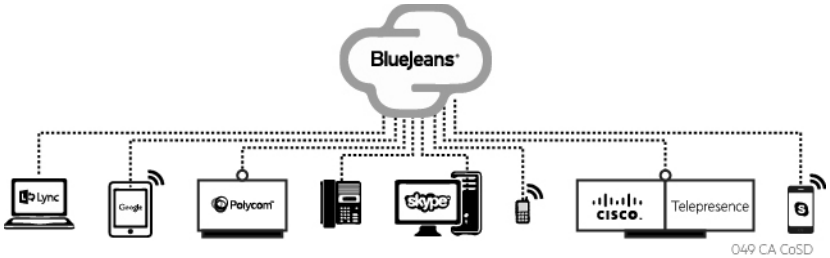
The members of this team will be identified by each framework as responsible for performance management in their discipline and will dedicate the necessary time to maintain a best in class performance analytics function. By taking early action, this team will drive through chronic issues and eventually reduce the effort for their resolution. Tools and practices, effectively used together, will increase the visibility of anomalies across the enterprise, improving the user experience while maximizing organizational performance and business output.

2.8.7. Describe your proposed approach for integration of desktops into Video Conferencing Services.

HPES currently provides room system based videoconferencing services for the County that leverage Cisco telepresence endpoints and a Tandberg/Cisco management infrastructure. While this infrastructure has historically been used primarily for point-to-point videoconferencing (both internal and external to the environment), the County has expressed interest in integrating this solution with desktop-based video capabilities.

An ideal integrated solution would enable onboard or peripheral camera devices to join multipoint conferences using either a web interface or Microsoft Lync (Skype for Business) Unified Communications client. This represents a unique challenge as Microsoft does not allow for a cloud hosted tenant to integrate directly with onsite infrastructure. To solve this problem, HPES proposes a solution based on AT&T Meetings with BlueJeans, a hosted video bridging capability that can integrate services such as Skype for Business and Google chat with traditional standards-based room video systems. This enables fully integrated business-to-business (B2B) video calling and is scalable, device and platform agnostic, and provides a flexible yet standard platform for video teleconferencing. Figure 91 illustrates this cloud-hosted service.

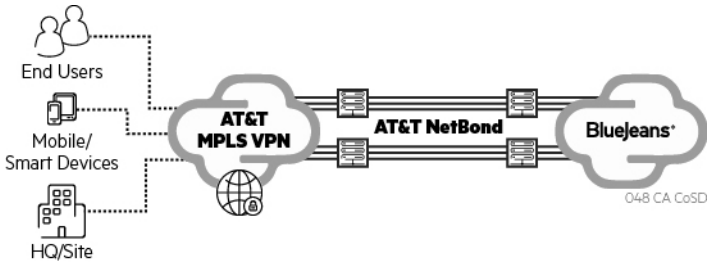
Figure 91. AT&T Meetings with BlueJeans



Cloud-hosted BlueJeans service provides multi-platform video teleconferencing integration.

Additionally, as the County increases its use of video teleconferencing, AT&T NetBond, as shown in Figure 92, will enable videoconferencing traffic to be redirected off of the ISP connections to a private multiprotocol label switching MPLS connection to support additional performance, scalability, and security above and beyond the integrated encryption. The NetBond to BlueJeans cost is not included in the Baseline Resources Units shown in Exhibit 16.1-1. As the demand grows and NetBond connection(s) to BlueJeans become warranted, the cost for the NetBond services would be determined from the proposed RUs shown in Exhibit 16.1-2 TF4 – Network tab.

Figure 92. BlueJeans Connectivity



AT&T NetBond-based connectivity to BlueJeans cloud effectively isolates video teleconferencing traffic across a secure, performance-assured AVPN connection.

This solution will integrate existing videoconferencing units around the County with Skype for Business clients, allowing for a more successful business collaboration with County partners and outside agencies. For example, this will enable video communication between the existing County VTC infrastructure and the Sheriff's Skype for Business based systems.

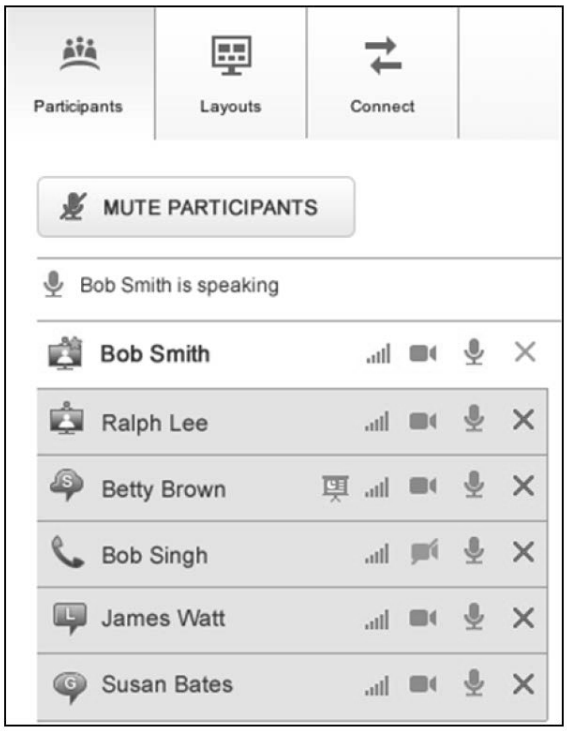
Mobility users can also participate in conferences using tablets and smart phones from anywhere, and on virtually any device through the use of a dedicated app, web browser, or the Skype for Business mobile application. Figure 93 illustrates various devices for conferencing.

Figure 93. BlueJeans Conferencing Solution

Users can use a variety of devices through the BlueJeans conferencing solution.

BlueJeans users can also benefit using Outlook plug-ins. A user can schedule meetings using a personal or dynamic meeting ID, edit default meeting preferences, and add, edit, or cancel meetings. Delegate scheduling provides administrative staff the ability to schedule meetings on behalf any team member. To set up a call, the user simply inputs the IP address as listed in the invite. Figure 94 illustrates email invites that include detailed instructions specific to each type of connection.

Figure 94. Email Invitations



Email invitation with detailed instructions helps users access conferences quickly and easily.

The BlueJeans platform allows numerous customizations including the ability to set language preferences, meeting passwords, entry tones, and meeting security controls via the web-based user interface. Features like high-definition content support, video sharing, and the ability to record meetings, coupled with the integrated encryption, provide secure meetings for County users.

In 2015, AT&T conducted a proof of concept exercise and was able to validate all functionality between the current environment and BlueJeans. This solution can be stood up in a matter of days if the County chooses to deploy this solution.

2.8.8. Describe your proposed approach for Town Hall Services.

The development of a video content distribution solution has been on the Network roadmap for more than 2 years, with the challenge being the identification of a solution capable of delivering a high quality, real-time, on-demand, and immersive end-user experience. HPES has evaluated multiple potential solutions with a focus on the following high-level requirements:

- Real-time video distribution to the entire enterprise (used for CAO or key informational addresses)
- Interactive capabilities to provide an immersive experience, such as voting, asking questions, among others
- Support for mobile devices including smartphones and tablets
- Capacity to support "County All" and scale as necessary
- The ability to support future deployment of on-demand video distribution to the enterprise (used for replay of videos)

HPES focused on three industry leaders in the video content distribution space. The following table provides a comparison of capabilities for three of these providers:

Feature	AT&T AVMS	Granicus	BlueJeans
Town Hall Real-time video distribution			
Capacity to support "County All" and scale as necessary	Yes	Over Internet Only	No, 5K limit
Internal Content Delivery Network (CDN) (Multicast Enabled)	Yes	No	No
External Content Delivery Network (CDN)	Yes	Yes	Yes
Combine live audio with PowerPoint slides and transmit to the audience's PCs	Yes	Yes	Yes
Audience can view the presentation and type in questions	Yes	No	No
Voting, polling options	Yes	No	No
Survey pop-up	Yes	No	No
Support Mobil Devices including Tablets	Yes	Yes	Yes
Optimize content viewing Bandwidth base on End Point Bandwidth	Yes	No	No
Provide and maintain webcasting equipment and infrastructure	Yes	Software only No Camera or Capture Equipment	Software only No Camera or Capture Equipment
Train users on processes related to conducting a successful audio webcast	Yes	No	No
Assist customers in the set-up, preparation, and launching of webcast events	Yes	Yes	Yes
Monitoring all Town Hall events a) Be online and available prior to event start time b) During the event be available for customer questions, troubleshooting, and solutioning c) Be available after event end to perform event completion steps and processes such as on-demand hosting and post-event customer questions	Yes	Unknown	Extra Fee
Manage customer event escalations	Yes	No	No
Video on Demand Town Hall and Archive distribution			
Prepare and post events for on-demand viewing. Provide archives.	Yes	Yes	No, Provide MP4 File
Assist customers with access to archived events.	Yes	Yes	Yes
Automatically archived and available for on-demand replay a few hours after the event	Yes	Yes	Yes
Archive is stored centrally and maintained for a minimum of one year	Retention set on per video basis	Unknown	No

Our first step in evaluating the field was an analysis of the existing Granicus video streaming solution (currently used for content external to the County network) to determine if it could be scaled to meet the requirements of the County's internal video distribution needs. We determined that while it would meet a subset of the County's requirements, it did not support multicast distribution within the enterprise. BlueJeans had the same internal content distribution limitation. This limitation would require significant infrastructure to distribute video and would represent a considerable impact to network bandwidth and performance. Additionally, both of these vendors also currently lack support for simultaneous, enterprise-wide viewership and have only provided intent to product road map the expansion of their solution to support the a network the size of the County's. Other vendors like Cisco (not pictured above) can support video solutions, but require infrastructure intense deployments across product lines and vendor platforms, increasing the complexity of integration efforts. In our view, this would result in an unacceptable level of management and in turn risk to the enterprise.

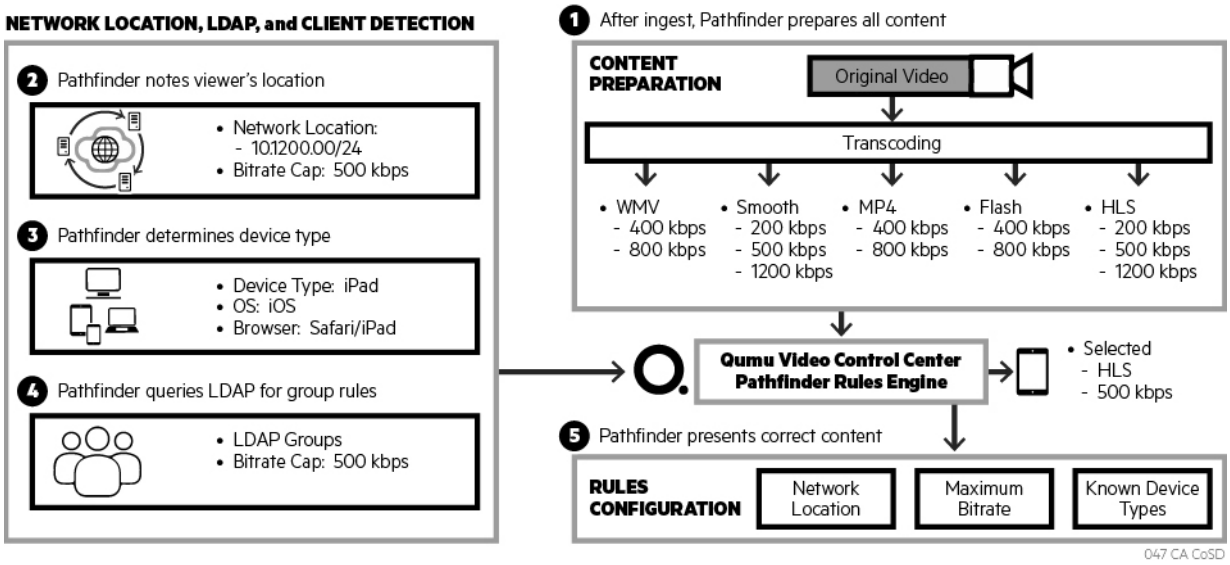
After analyzing these provider options, HPES recommends AT&T Video Management Services (AVMS) to provide town hall video services for the County. AT&T and its partner Qumu are uniquely positioned in the industry to deliver high quality live and video on demand services. Qumu is ranked within the upper right of the Gartner Magic Quadrant for Enterprise Video Content Management based on their robust streaming architecture and unique ability to address the widest variety of customer implementation models, from on premise to hybrid or private cloud. This platform, coupled interactive functionality, provided tools and analytics capabilities, and custom support arrangements, gives Qumu the ability to tailor their video solutions to meet its customer's specific needs.

AVMS provides all of the functionality needed to capture, manage, and publish video content for both live and video on-demand (VoD) distribution for local and remote users. AVMS's advanced transcoding capabilities support formats from various capture devices—from production studio and video conferencing platforms to mobile devices and video cameras. This provides the capability to transcode to numerous video types and resolutions to support multitudes of devices simultaneously, such as H.264 x 480 for mobile devices and H.264 x 720 for desktops. For distribution, the solution allows for

consumption of video content on a wide variety of devices such as laptops, desktops, tablets, and smartphones while optimizing the user experience based on the device being used and bandwidth available.

By means of Pathfinder, AVMS' intelligent routing and distribution element, the system is able to optimize and present content viewing based on device, network location, and bandwidth, as illustrated in Figure 95.

Figure 95. Optimization of Content Viewing



The ability to create subdomains will provide separate access to video intended solely for users on the County domain, such as internal communications or training. Internal and mobile video viewing can even be limited to specific groups based on AD group.

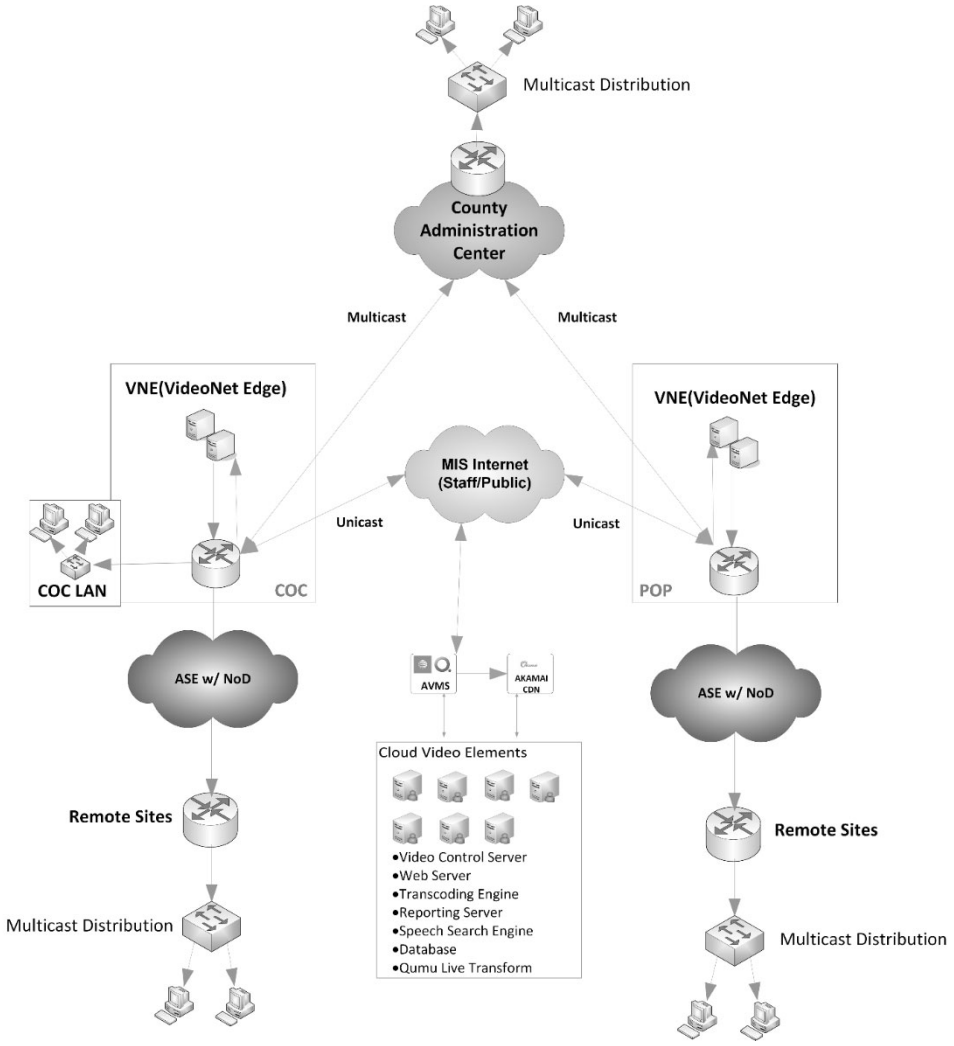
Embedded polling and feedback features offer increased benefit to the County by engaging viewers and soliciting their input. High grade analytics will provide viewer statistics along with broadcast performance detail to provide a clear picture of content performance and identification of possible impacts.

AVMS offers both on-premises and cloud-based options. The HPES team recommends the cloud-based architecture which provides high availability without the need for extensive local hardware and associated support costs. With the added benefit of burst capacity for mobile or public users in real-time, the solution is able to handle traffic spikes without degradation of the delivery quality. The hosted solution can scale to cover all of the county users with growth up to 100,000 simultaneous viewers. With archiving capabilities, video content can be preserved and made available for replay for a configurable length of time.

AVMS makes use of both internal and external Content Delivery Network (CDN) technology. For external content delivery, the Akamai platform is leveraged. This external content delivery capability could also be used to augment or potentially replace the Granicus streaming solution.

From within the County domain, the AVMS solution enables multicast video presentation through VNE's (VideoNet edge) to multiple viewers simultaneously without causing an exponential impact to network performance. We are recommending four VNEs, two at COC and two at POP. From this geo-redundant core, the multicast stream can be routed across the WAN to the remote edge, where the LAN redistributes the stream to each requesting user.

Figure 96. AVMS Topology



Topology of the AVMS solution, highlighting cloud based services feeding geo-redundant Video Network Edge devices that feed multicast video streams to the remote County sites.

The HPES team can also provide the video capture components and production services necessary to deliver video content from start to finish. We recommend making video and audio capture equipment available through the OIC catalog. This capture capability can also be augmented through the use of customized production services, providing a range of capabilities, including onsite support, on a "per event" professional services basis which is not included in the proposed Resource Unit. (This will ensure these event specific enhancements are paid for by the business unit or department utilizing the services.)

In order to represent a complete solution with no limitations to the County, HPES is only proposing AVMS for enterprise video content distribution. Our proposal includes a fixed monthly resource unit charge for an unlimited number of townhall events which can be allocated to business units based upon the County's discretion. Upon agreement, HPES will work to implement this service between CED +180 and CED+360.

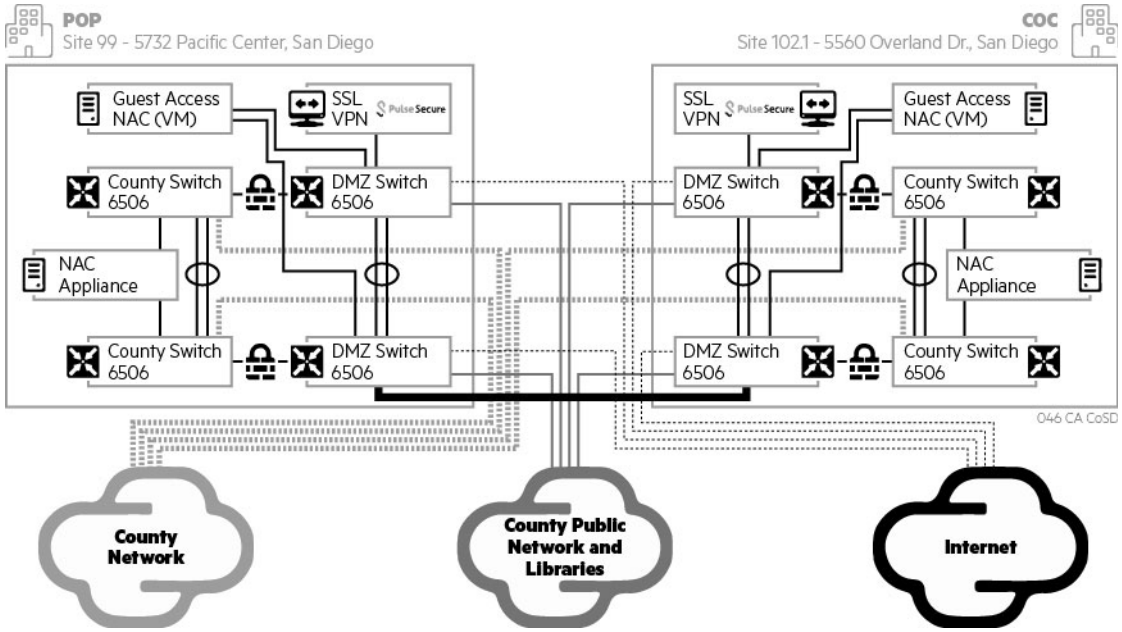
Video is the future of corporate communications, as evidenced by its extensive use in the private sector by large fortune 50 companies. With an enterprise the size of the County of San Diego, the opportunities that this technology represents are extensive. The AVMS solution proposed by the HPES team is structured to

grow with the County's needs, however it is most cost effective at an enterprise scale with heavy adoption from the business units. With a directed push by County leadership in the utilization of this technology, the County could place itself in an elite position as an early adopter amongst its peers. This service will enhance directed communications to County employees, improving employee engagement and opening yet untapped pockets of productivity. Our solution provides features and benefits that will allow the County to be at the forefront of technology for local Government IT organizations by providing a "best in class" video content delivery solution for its employees and constituents.

2.8.9. Describe your proposed approach for network access controls and PKI-based device authentication for Wireless Services.

Network access control (NAC) is a key milestone in the network framework security roadmap. After an extensive evaluation of the top two vendors (Cisco and Aruba), including proof of concept efforts, HPES determined that the best-of-breed product to provide a comprehensive yet integrated NAC solution is Aruba's Clear Pass Policy Manager (CPPM). This product will provide the County all the features of NAC in a single platform to ease management Figure 97, administration, and troubleshooting efforts. An integrated RADIUS server, coupled with the ability to perform guest access authentication, will provide a wireless solution enabling County staff and the public appropriate, policy based network access across any access point in the County. This will provide a seamless authentication for the staff while allowing various options for the redirection of public or untrusted devices. While the wireless deployment is planned to be implemented first, HPES proposes the solution to function on all physical ports Countywide.

Figure 97. NAC/Guest Access



NAC/Guest Access centralized management topology is provided via a geo-redundant architecture.

The Aruba NAC solution will be implemented to align with our geo-redundant, high availability standard. One appliance will be located at the AT&T POP and one installed at the County Operations Center (COC). These appliances will manage and enforce policy on the staff wired and wireless infrastructure by leveraging 802.1X and EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).

The solution will allow any County domain joined device that is plugged into the network, and logged into with a valid active directory account, to be given access to County network resources. Any devices plugged into the wired network that do not meet the above criteria, or predefined NAC policies for nondomain joined or non-dot1x compliant devices, will be placed onto a public VLAN with restrictions that allow for access to the Internet only.

The integration with the existing wireless infrastructure will continue to leverage EAP-TLS to validate certificates for access to the existing County secure wireless network. The certificate required to authenticate, as well as the wireless profile, are installed at the time a computing device is prepared for distribution by means of a group policy object (GPO) push within the desktop framework. This GPO is the only way the client machines can receive the certificate required.

To provide public guest access, the HPES team proposes installing a virtual instance of a clear pass policy manager in the DMZ at both the AT&T POP and the COC for redundancy and resiliency. This will provide guest access on the public Wired/Wi-Fi network. The solution will force all users of the public network to view the captive portal splash page where terms and conditions can be presented and must be accepted prior to being granted access to the Internet, as shown in Figure 98. The contents of the splash page, as well as the look and feel (theme), can be modified to include desired content or photos and provide automatic forwarding, after acceptance of terms and conditions, to the County's home page.

Figure 98. County of San Diego Splash Page

Public guest access login page can be modified to provide an enterprise standard user experience, including the placement of the County seal or graphic backgrounds.

This guest access solution also offers functionality that could be leveraged for business unit specific use cases. As an example, the County libraries have expressed an interest in using a registered library card number as a requirement to allow Internet access. Aruba's ClearPass Policy Manager Guest access solution possesses the ability to integrate various types of databases or data stores and use them for authentication credential purposes. This has the potential to give the County libraries the ability to restrict access based on the issuance of a library card, in turn driving constituent registration, a key element the library group uses to track and represent the value of their services.

AT&T currently maintains a RADIUS serve (steel belted radius [SBR]) that acts to authenticate radius sessions from the wireless network. The HPES team proposes leveraging the two Aruba appliances planned to be installed at the AT&T POP and the COC to provide radius server functionality in place of the existing SBR server. The two appliances will be fully redundant thereby removing a single point of failure and provide all services currently offered by SBR. HPES may integrate the new radius servers with the existing Microsoft CA infrastructure as well as the new Symantec-managed PKI solution to minimize disruption and support our cross functional framework activities.

Generally, staff users will be unaware of any additional security when using a managed County computing asset. The EAP (Extensible Authentication Protocol) required to validate the user and machine will leverage currently logged-in user credentials and domain membership to allow access.

Strategically NAC provides another layer of defense in depth strategy the County and AT&T have employed for years. By leveraging NAC as the first layer of defense protecting at the lowest points in the OSI model, other measures including IDP/IDS, security policy, and access restriction can be tuned to greater efficiency and provide additional layers necessary to fully realize the merit of a layered strategy.

2.8.10. Do you have any alternative approaches to New Site Installation for County consideration?

HPES has responded to the County's desire to replace the existing new site installation process with an approach that is compliant with the stated requirements in this RFP. One approach for the County to consider an additional resource unit that covers those sites containing between 1 and 10 County users.

During the past decade, there were more than 50 new sites (for a total of 87) built by the County that housed 10 or fewer occupants. These sites include fire stations, road maintenance yards, telepsychiatry offices, ranger stations, and other small County facilities. The proposed new site standards would include these sites in the same resource unit as locations with as many as 50 users and will carry a hefty price tag due to its association with much larger sites in the range. We believe that the addition of one more resource unit, sized for sites between 1 and 10 users, will more closely connect cost and price for these new locations and remove a potential financial burden for the County in the construction of smaller sites.

Network Services Framework – Executive Summary

The County can minimize risk and maximize improvements to its infrastructure by retaining HPES. We currently provide end-to-end network services that are continuously improved and transformed according to jointly agreed to strategic roadmaps. During the past 10 years, we have worked with the County to build a network with maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest reliability, security, and service levels. As a result of this successful collaboration, we have transformed the core network to eliminate single points of failure, improve disaster recovery capabilities, and expand end-user functionality. And, we have developed strategic plans to further improve the County's network performance.

Key Differentiators

Our team offers four critical differentiators:

- **Institutional and operational knowledge** that is impossible to acquire without years of experience. Your Network Lifecycle Management Team has an average of nine years of experience supporting the County's network. They keep their skills current through annual training programs tailored to their area of expertise—our team currently holds 34 different certification types covering all aspects of our framework. Your Network Team also has access to a "deep bench" of technical resources through our Centers of Excellence. Combined with our knowledge of the County's network, our technical expertise leads to better performance and more productive transformation roadmaps. With your existing team,

it's personal – we live and work in San Diego and we have a vested interest in making the County's operations the best in the nation.
- Selecting our team will **eliminate network transition risk**. Rather than worry about the time and expense of shifting operations to a new provider, the County can remain focused on its transformation initiatives with a team that has already proven that it can execute on its commitments.
- We have a **track record of tight integration** within and across frameworks. Our team has integrated service management processes to provide quick resolution to problems and clear escalation paths. We manage joint requests as a single team, including architecture, planning, and governance. This integration has helped us achieve perfect service levels with the County for the past 30 months, and near-perfect performance for the past 10 years. We maintain high reliability and progressively improve our teaming arrangement for the benefit of the County.
- Finally, our team can provide services based on the latest developments in **cloud-enabled and software-defined networking**. Unlike other providers, our services and management tools are fully tested by AT&T Labs for reliability and interoperability. The County of San Diego can be confident that these emerging technologies will work as intended in its high-volume, mission-critical environment.

Transformative Governance

The HPES Network team has implemented a customized approach to transformation that has set a new standard in its effectiveness and ability to align with County strategy. At the foundation of this approach is a close collaboration with the County Technology Office and the HPES Enterprise Architecture Team where technical leadership meets weekly to discuss strategic objectives and the industry drivers influencing solutions to business problems.

Our team supports the County's transformation objectives through careful long-term planning and creative use of refresh technologies and capital resources. In fact, we often incorporate new functionality into existing services at no increase in the RU price. This approach allows us to support growth while effectively managing risk to your enterprise.

Transformation Opportunities

We have identified several transformation opportunities that can improve the County's operations. As software defined network and cloud-based services mature and become more viable for government use, we are positioning the County's network to take advantage of these new services. For example, we are currently working with the County to support the following initiatives:

- **AT&T Switched Ethernet (ASE) with Network on Demand:** Migrate 115 Opt-E-MAN sites and approximately 80-90% of T1 sites to ASE w/ NoD. This service will provide much faster installation and near-real-time bandwidth scaling, as well as improvements in reliability associated with new software defined transport infrastructure and fiber for the T1s. This solution will also allow for more bandwidth at the same or reduced costs relative to the County's existing Opt-E-MAN service.
- **GigaMAN backbone consolidation:** Redesign the Gigabit backbone from six to three sites. This consolidation improves security inspection points, provides least-cost/shortest-path to services (Internet or data center), and maintains redundancy for key County facilities.
- **Datacenter Connectivity:** Provide connectivity to the new consolidated datacenter using geo-redundant MPLS transport. This service will provide the County with higher bandwidth and increased flexibility to dynamically shift workloads to the fail-over datacenter if needed.
- **Office 365 NetBond:** Provide NetBond connectivity to Office 365 for Exchange/Lync. Using geo-redundant AVPN connectivity, the NetBond service provides secure, performance-assured connectivity to your cloud-based resources and offloads critical business traffic from your ISP links. A new NetBond Resource Unit will also enable future adoption of cloud services.

- **Voice over IP to the desktop:** Migrate more than 13,000 Avaya time division multiplexing (TDM) voice users to the existing Avaya VoIP core, replace digital handsets with Session Initiation Protocol (SIP) handsets, and enable RedSky E911 at all VoIP sites. This solution improves long-term reliability of the voice network by eliminating end-of-support/end-of-life equipment while improving the user experience.
- **Unified Communications (UC):** Integrate HPES-supported Skype for Business with AT&T-supported Avaya enterprise voice infrastructure. This solution improves end-user productivity through real-time communications via a single, integrated desktop client.
- **Expand SIP services:** Expand SIP trunks to support long distance and toll services, eliminating usage based charges in these legacy resource units and substantially reduce Toll Free 800 usage rates. We will continue to evaluate additional services that can use SIP signaling to support the overall enterprise voice and unified communications services.
- **Centrex to VoIP:** Migrate Centrex to VoIP where possible, by leveraging existing data network connectivity. By aligning with the enterprise VoIP and UC standard, we can increase capabilities to remote stations.

We're also in the evaluation and planning stages for the following transformation opportunities:

- **Eliminate T1s:** Identify isolated T1 sites where fiber is not feasible and evaluate solutions using copper based AVPN or mobility Commercial Connectivity Services (CCS LTE).
- **Eliminate Centrex:** Migrate non data connected Centrex sites to suitable replacement technology, including potentially leveraging the mobility network for services.
- **Pilot universal Customer Premises Equipment (uCPE):** Trial and test uCPE in preparation for potential mid-term transformation of sites in line with refresh investments. Universal CPE will allow the County to provision new services and orchestrate changes to its network functions in near-real-time.

As the needs of the County evolve, our team will continue to collaborate with business units, County Technology Office staff, and our cross-framework alliances to understand your challenges and develop effective solutions. Transformation is an iterative process, requiring strategic planning and vision combined with practical approaches that focus on ensuring that the County gets access to new functionality in the most expedient way possible. The technologies identified in this solution are just the beginning of a contract lifecycle of change that will provide a foundation for growth as we move forward as a trusted advisor to the County.

The Future of the Network: Software-Defined and Virtualized

We have made significant investments to begin transforming our core network and services to a software-defined and cloud-based delivery model. By 2020, we plan to virtualize and control more than 75 percent of our core carrier network using this new SDN architecture. Our vision for the future eliminates proprietary network hardware and allows applications to be downloaded onto a virtual machine and programmed via an application programming interface (API). SDN-enabled services will provide the County with the following benefits:

- Network and service simplification—with no additional equipment required for new services, an asset-less office becomes possible and equipment purchase and maintenance costs can be reduced or eliminated
- Near real-time service provisioning or changes using APIs
- Integration and automation to reduce administration and configuration efforts
- Increased security with software residing in the cloud
- Greater access to data for analytics

This initiative helps us control and configure our own network, and it also sets the stage for customer-facing services. For example, we are moving network functions from hardware to software elements that can be dynamically instantiated on universal CPE, either in a cloud-based data center or on a customer's premises.

Our investment in NFV, SDN and cloud technologies will change the traditional approach to network management, security, and cross-functional operations. We're creating an ecosystem of services that can help the County lower life cycle costs, speed application delivery, and facilitate new IT functions. Services of particular interest to the County include:

- **NetBond:** We are positioning the County's network perimeter for secure and performance-assured integration to cloud providers. Using AT&T's VPN service as a private network connection, we can isolate traffic to these important services, removing them from the unsecure and potentially congestion-prone ISP links. Building on the existing AT&T VPN transport, we will use NetBond service to terminate at the County's edge, providing a geo-redundant presence coupled with the inherent redundancy of the global AT&T MPLS infrastructure. This design will provide the highest level of resiliency available to ensure the County's ability to conduct business.
- **Network on Demand:** Our first SDN-enabled network service, launched in 2014, can help the County increase or decrease its network bandwidth as needed in near-real time. The County's first SDN-enabled services were implemented at two sites in 2015, followed by a new site standard implemented in January of 2016. Currently six County sites are utilizing this new technology in production. We plan to leverage this new standard by migrating existing Ethernet and T1s to AT&T Switched Ethernet with Network on Demand. This service will provide much faster installation and near-real-time bandwidth scaling and improved reliability inherent in fiber based services.

Universal CPE: We have worked with our suppliers to decouple their software from their proprietary hardware, creating a 'white-label' x86 appliance (Universal CPE or uCPE) that acts as a customer site virtual machine. By using a simple, standardized machine to perform a variety of network functions, and shifting the capital costs to the provider, we can greatly reduce your total cost of ownership (TCO).

County Benefits

The County has consistently ranked as one of the highest in the nation in the Center for Digital Government survey of the effectiveness of digital services for large counties (http://www.govtech.com/dc/articles/Digital-Counties-Survey-2015-Results.html). Our team has supported the County in this achievement by serving as a consultant at every step of its network evolution. Today, we help the County maintain currency and consistency across the network and confidently adopt new technologies and capabilities. With our advances in software defined networking and network function virtualization, we will become even more efficient at serving the County's needs.

The IT framework synergy needed in an enterprise the size of the County requires teams that work together well, have significant resource depth and breadth, and provide maximum organizational agility. Our team has continuously refined its organizational model for fully outsourced network services. Using local resources in a dedicated support model that truly augments the County's team, we actively collaborate with other framework providers toward common operational and strategic objectives. This organizational model, combined with our extensive experience cooperating in large outsourcing environments, delivers optimized, best-in-class options for IT outsourcing.

By selecting HPES and our partner AT&T, the County can reduce the risks that often accompany transition to a new provider—for example, time and money spent performing knowledge transfer and site transitions. Instead, the County can continue to focus on its agenda for transformation and IT excellence.

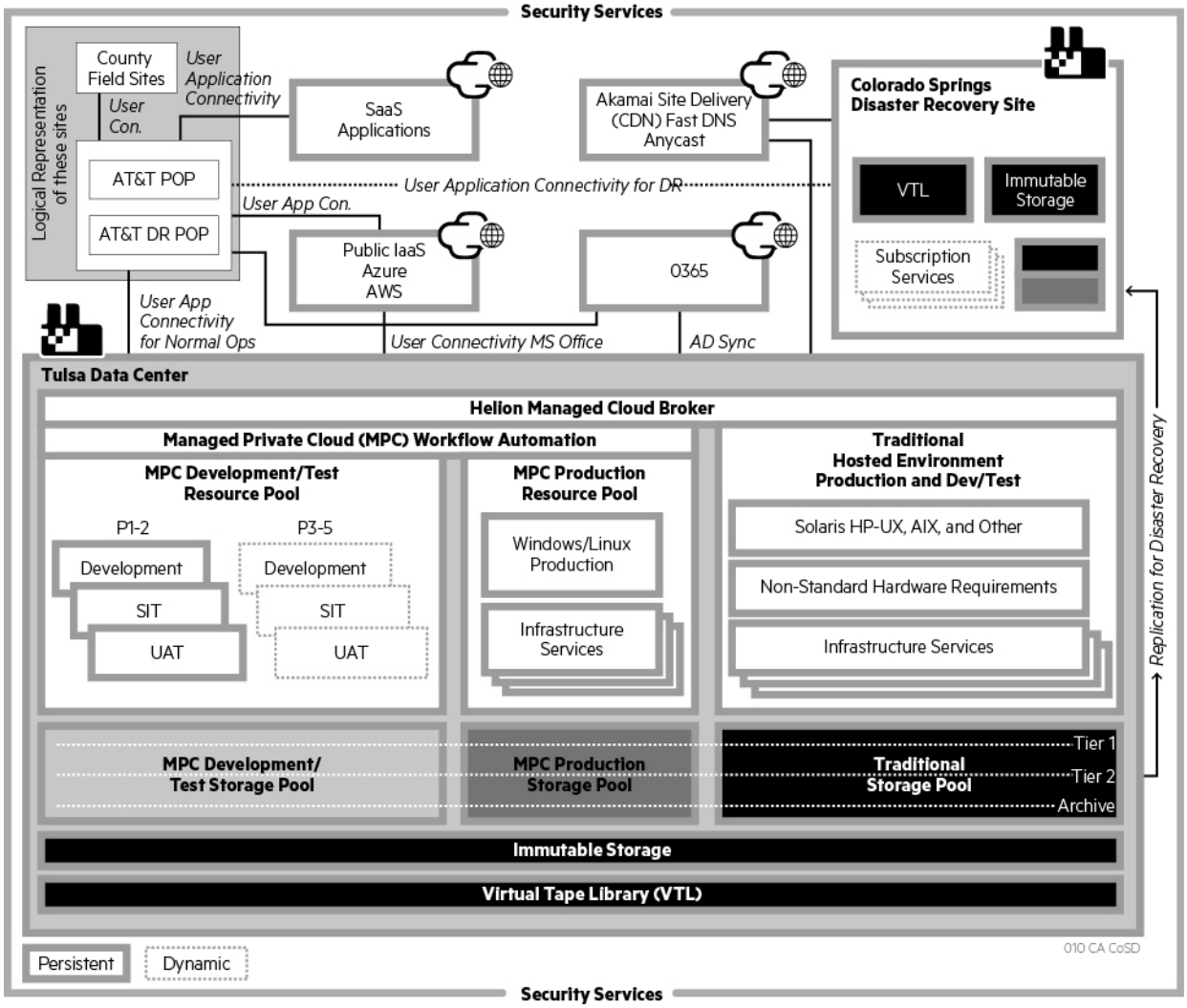
HPES has demonstrated our commitment to the ongoing transformation of the County's network. The model for local Government IT outsourcing was pioneered by the County, with HPES as a trusted advisor in every engagement since its inception. We can continue to apply our experience, vision, and knowledge to help the County use advanced technology to support its constituents and community. HPES is best positioned to provide the virtualized, cloud-based services that will define the County's future network. We look forward to strengthening our relationship and contributing to the County's ongoing success.

2.9 Data Center Services Framework

Executive Overview

Reliable, predictable, and secure information technology services play a critical role in helping the County efficiently provide services to the public and deliver with operational excellence. With its outward focus on supporting healthy families and safe communities, a recognized and trusted technology partner is critical to build, manage, and operate the underlying infrastructure that supports the County's business processes and applications. HP Enterprise Services, LLC (HPES), has designed a data center services framework solution, shown in Figure 99. , to fully meet the County's needs and facilitate consolidation of applications and infrastructure services into a single Tier 3 production data center in Tulsa, OK, where the majority of the County's applications currently reside. This facility is ISO 9001:2008 certified and meets stringent public sector compliance and security requirements. Each element in Figure 99 is described in our response to the data center service framework component sections below.

Figure 99. HPES data center Services Framework Solution

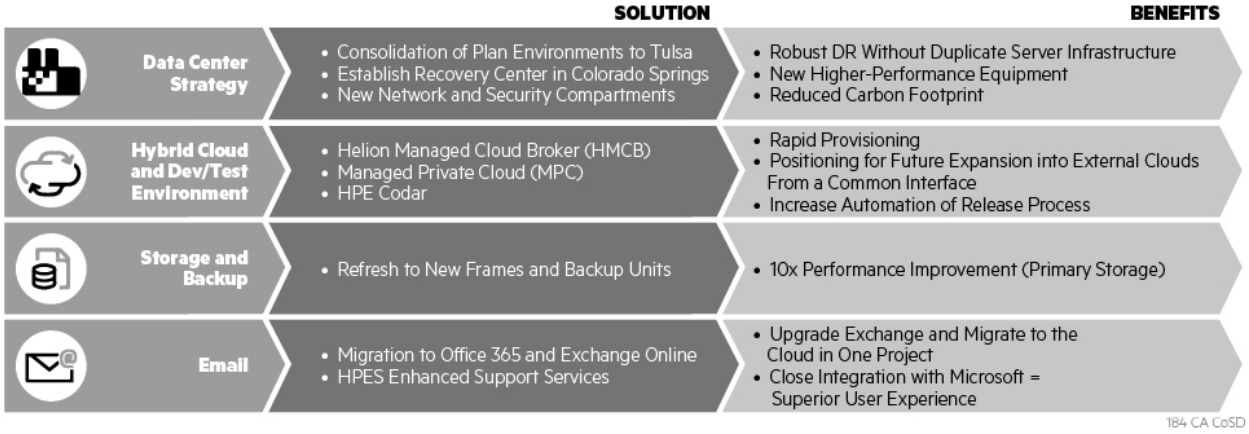


HPES' robust data center services framework solution will meet the County's needs and requirements to consolidate data center services in Tulsa.

Framework Components

The proposed data center strategy and its benefits are summarized in Figure 100.

Figure 100. Data Center Solution Key Benefits

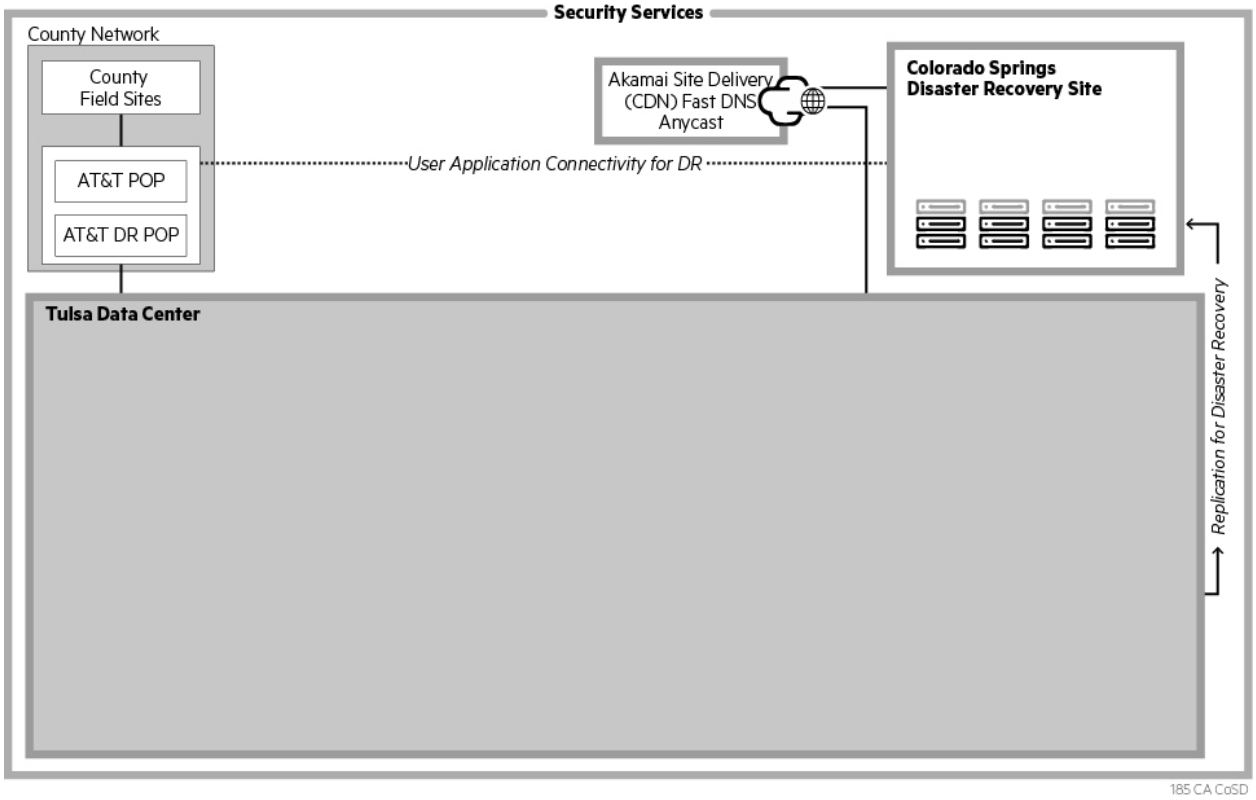


Our Data Center Framework strategy positions the County for the next wave of IT services as well as making some of those services a reality right away.

- With advances in technology, we no longer have to have dual primary data centers to have a robust Disaster Recovery (DR) strategy—you can position services in our recovery center without duplicating your production server environment.
- We will put in all of the building blocks to move you into the cloud, within the data center, as well as positioning you for the next wave of cloud services—whenever you are ready to take that step.
- We will bring in the latest in data center network, security, storage, and backup technology.
- Your email upgrade will be much more than just an upgrade—we will help you get all you can from your Microsoft Office 365 licensing, from Exchange Online to OneDrive for Business to SharePoint Online. To make sure this experience is a good one for the County users, we have included our managed services, so that the support experience will be the same as if we were managing a local service.

Figure 101 illustrates the end state for the Data Center Framework, following the Data Center Transition. The following sections describe each part of this diagram.

Figure 101. Data Center Facility Strategy



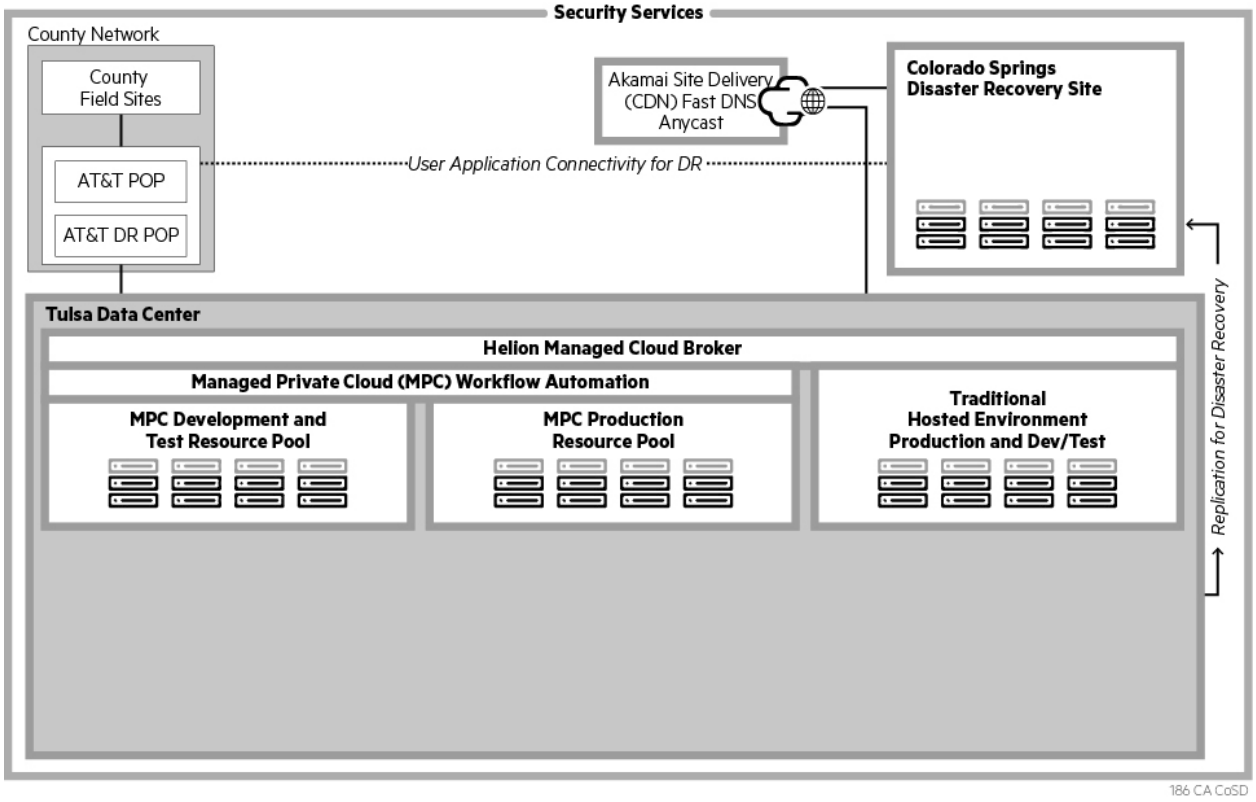
Two primary sites are no longer required for rapid recovery: our solution provides a consolidated site and a highly flexible and secure Disaster Recovery site.

Our Data Center facility approach is to consolidate all of your primary workload into Tulsa, and set up a subscription-based DR service in Colorado Springs. Some of the benefits of our DR solution follow – the solution itself is described in more detail in Section 2.5.

- Reduced complexity in architecture: Technology has evolved to the point that dual primary data centers are not required to provide robust DR – we can focus high availability in the primary site and have the ability to meet your recovery time objectives/recovery point objectives (RTOs/RPOs) with a subscription-based DR solution.
- Colorado Springs is an HPES Next-Generation facility, which means it employs all of the latest green technologies; itis highly secure (between the outside and the data center, a person has to pass six levels of badge entry and one biometric reader); and staff follow all of the same processes as in our other data centers, providing consistency of results and quality support.
- We will still leverage the investment in Akamai Domain Name System (DNS) services to facilitate site redirects when needed, as shown.
- We have added resources who are experts in DR planning and testing who will focus on this area and have testing methods that will enable you to perform more accurate recovery testing than table-top exercises (although we will still do table-top exercises when appropriate), without having to take down the production environment to simulate a disaster.
- The new network compartment that we build inside of these two data centers will have the latest high-performance equipment, and we will replace the current Checkpoint/TippingPoint configuration for firewall and Intrusion Prevention/Detection with Palo Alto units that will perform both functions. We have had great success with other large data center clients on this platform, and this aligns with AT&T's strategy of using Palo Altos on the County network.

The Transition Project Manager responsible for the Data Center Consolidation and buildout of the DR environment will coordinate with HPES' Continuity Services organization to build out the DR network compartment and acquire the dedicated equipment for the County's DR environment. They will also establish subscription services for those applications that have DR requirements. Because subscription services are leveraged by nature, these services are already part of the Continuity Services inventory and are available to the County for use during DR testing or a DR event. The Continuity Services organization provides capacity planning and procurement as needed for this service as part of the subscription onboarding process. Servers in the managed private cloud (MPC) environment that require DR counterparts will have subscriptions based on our Enhanced Disaster Recovery service, which is a virtual private cloud. Figure 102 illustrates our hybrid cloud architecture.

Figure 102. Hybrid Cloud Architecture



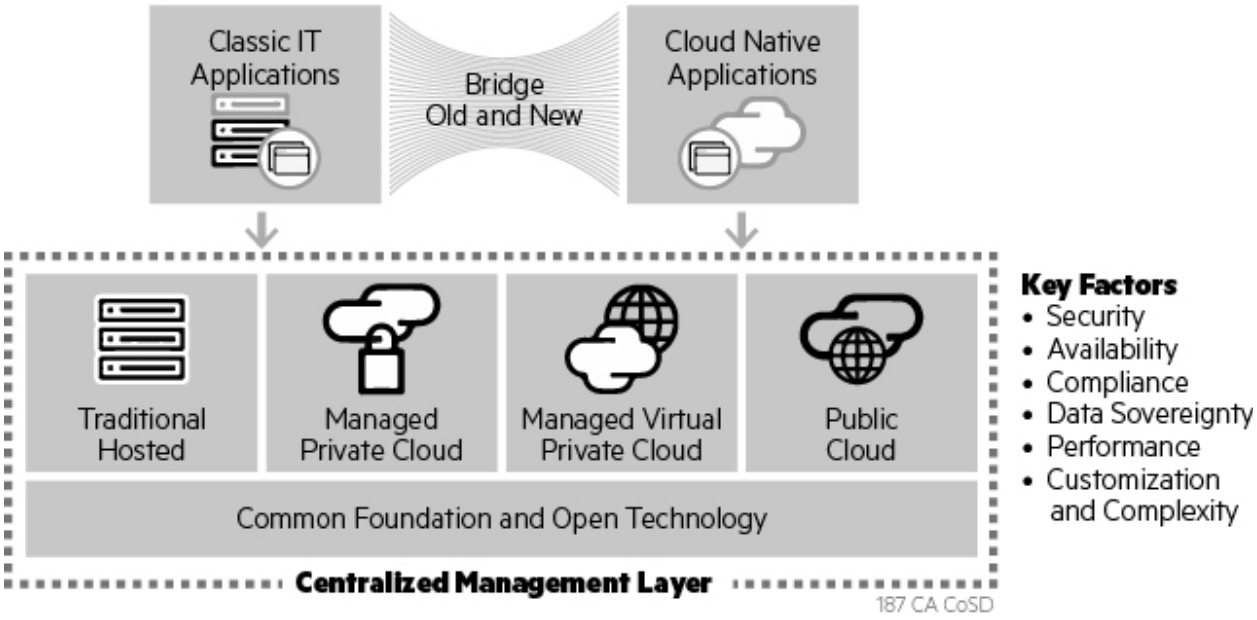
The Hybrid Cloud solution provides extensibility into future cloud services while making some of the benefits of cloud services available today.

The Hybrid Cloud architecture consists of the following:

- The Traditional Hosting Environment—essentially the services you have today
- A Managed Private Cloud (MPC)
- The Helion Managed Cloud Broker (HMCB).

All three types of servers—Applications, Development and Test, and Infrastructure Services—can have some server presence in both the MPC and the traditional hosting environment. The reason for having both is to enable the County and HPES to choose the most appropriate architecture for the needs of each application. We illustrate this continuum of services in Figure 103.

Figure 103. Continuum of Classic IT to Cloud Native Architecture Choices



Choose the right architecture to meet each application's needs, but manage them as an integrated whole.

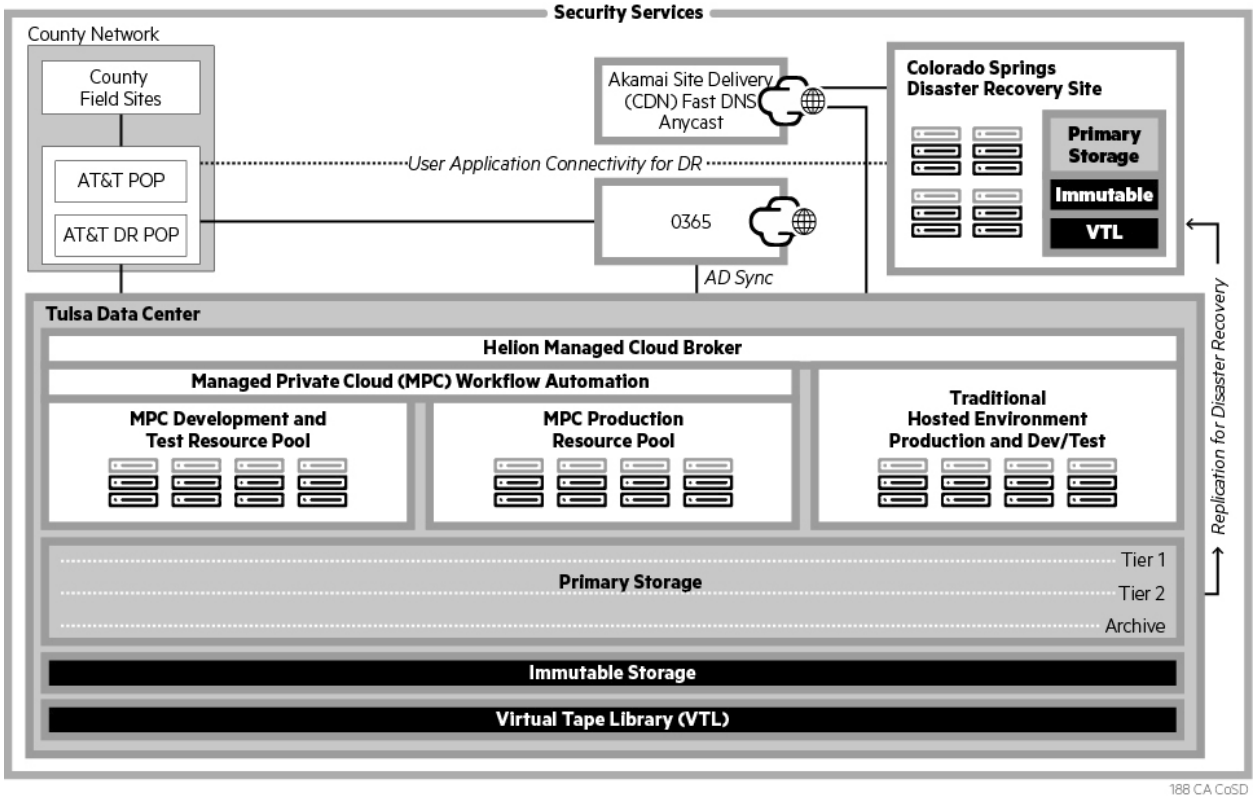
The factors shown above illustrate the drivers for choosing one type of environment over another. Higher levels of security, customization, complexity, etc., are factors that would likely favor the Traditional Hosted side of the spectrum. "Cloud native" applications are, by nature, more encapsulated and less tightly integrated to a particular platform architecture. For each of the County's applications, we have performed a preliminary analysis of hosting choice between the Traditional and MPC environments. The criteria for moving an application's environment, either in whole or in part, into the MPC, plus a list of applications that meet that criteria, are fully described in Application Infrastructure Services (Sched. 4.3, Section 6.7). Note, however, that migration to the MPC for production environments will be considered, at the County's discretion, upon refresh, rather than during Transition. A full discussion of the Development and Test environment approach, including the rationale for having persistent server environments for certain P1/P2 application servers, appears in Development and Test Services (Sched. 4.3, Section 6.9).

As the County's applications estate moves toward more cloud native applications, we include the option to provision into virtual private and public clouds when you are ready. This capability is included as an optional additional Resource Unit (RU) but does not require any new development to implement; it is available with the solution provided in Transition. Also note that our Data Center Transition plan does not include migration of any environments into public or virtual private clouds at this time.

The key to adding value in a hybrid environment, rather than having a bunch of soloed service providers, is to have a centralized management layer that provides visibility and control into all of these providers, as depicted above. That centralized management layer is the HMCB.

The final piece of the picture is the Storage Services environment, including Backup and Recovery services, as illustrated in Figure 104. These services are described in detail in Storage Services (Sched. 4.3, Section 6.12).

Figure 104. Storage Services



A common storage environment is deployed across the cloud, traditional, and DR environments.

Details of how these services are implemented during the Transition period are provided in Section 2.11 – Transition Services, Consolidated, and Single Data Center, Section 3.4.

Security Services (Sched. 4.3, Section 6.5)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The proposed data center solution will consolidate all services from Plano TX and Tulsa into a single production data center in Tulsa. The new environment will incorporate a Managed Private Cloud (MPC) environment for development/test (Dev/Test) services, and retain the traditional hosting infrastructure for production applications and those that are not cloud compatible. It will include the deployment of firewalls, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) devices, host-based security and full spectrum analysis of all traffic in and out of the Tulsa data center. Our solution incorporates robust IT security within the Tulsa data center, to meet the specified requirements. Our approach to data center security involves disrupting the entire life cycle of an attack, by investing in both layered prevention and detection, and in a network configuration that creates separate security zones.

Rationale: This defense-in-depth approach results in real-time threat disruption to an adversary attempting to attack County infrastructure and applications housed in the HPES data center. We honed this approach through our work with every major branch of the DoD and will apply this experience to provide a robust security solution to the County. The HPES solution includes:

- **Implementation of Palo Alto next generation firewalls.** These multifunction devices provide firewall services, intrusion prevention and detection services, spyware and antivirus filtering, web content

filtering as well as unified threat management capabilities. This solution also provides automated alerting of possible malicious activity and daily threat updates.

- **Network zone restructuring.** The County has three network architecture tiers—Front DMZ, isolation zone, and data center zone. The production zones are implemented by a combination of network segmentation, device separation, and firewall separation between each zone. The Dev/Test environment has virtual local area networks (VLANs) representing each of the three zones. However, currently, all VLANs are located in the data center zone, and traffic from the Dev/Test environment has unfettered access to the production VLANs in the data center zone. This poses a security risk. The Dev/Test environment will mimic the production environment. That is, VLANs for Dev/Test will be located in each of the zones (front DMZ, data center zone and isolation zone). The Dev/Test VLANs will be segregated from the production VLANs by the firewall and will not have access to the production VLANs unless access to specific Services are required (e.g., Active Directory). If a firewall change is required by M&O activity, all labor associated to the firewall change will be covered under Apps M&O. In addition to eliminating the security risk, it will provide for more comprehensive application testing. With the current configuration, applications test firewall rules associated with the applications in the test/dev environment since all are in the same zone. With the restructuring, applications will be able to test firewall rules earlier in the process and hone during testing. This will facilitate a cleaner cutover to production.
- **Expansion of ArcSight Security Information and Event Management (SIEM) Services.** Currently, all firewalls and IPS sensors, VPN devices, and DHCP appliances in San Diego, Plano, and Tulsa are enrolled in SIEM services (log collection, log management, and reporting as well as 24x7 alerting and monitoring services). In addition we will include "critical servers" such as domain controllers or servers with data subject to regulatory compliance, such as HIPAA and PCI.
- **Email Security.** With the transition of email to the cloud, email-specific security services will be provided by the Exchange Online Protection (EOP) capability, which provides comparable security services to the IronPort appliances, such as:
  - Data Loss Prevention (DLP) for email
  - Advanced Threat Protection (ATP)
  - Exchange Online Archiving for Exchange Online
  - Legal Hold
  - Antispam/Antimalware at the mailbox level

- **Distributed Denial of Service (DDOS).** DDOS protection is a prime example of defense in depth. It includes protection at the Internet Service Provider (ISP) layer outside of the County environment, firewall configurations, network configurations, Access Control Lists (ACLs), intrusion prevention system configurations, Web/DNS traffic DDOS protection provided by Akamai, endpoint protection on all windows systems, operating system hardening, browser protection as well as application level protections.
- **Active Directory.** HPES reviewed the current AD2012 solution to validate that the integrity of the design will not change with the data center consolidation. The following components will be re-engineered as part of the consolidation during transition:
  - Domain controller redundancy standards (rule of three) for the CO domain
  - Flexible single master operation (FSMO) roles failover locations for CO and County domains

- HPES will also implement the following tools:
  - **Dell Recovery Manager Active Directory (RMAD)**. RMAD functionality includes the restoration of deleted objects as well as corrupted objects and provides the ability to recover an entire domain or forest in the event either of these is lost or corrupted. RMAD eliminates the need to recreate impacted objects and results in quicker service restoration.
  - **Dell Enterprise Reporter**. Enterprise Reporter provides reports related to Active Directory, which will provide the County to better monitor and manage user access and respond to audits.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES will support security services using a combination of resources dedicated to the County and HPES corporate resources with specific areas of expertise. These include the HPES CISO, HPES Security Operations Manager and leads for the various functional areas (threat management, access management, security engineering, and risk management among others). The HPES security teams will provide the daily support of the various security services and security infrastructure components based on their area of expertise.

HPES security staff will be located at the following sites to support the County, so that we can continue to work closely with the County CIO, CISO, CTO and supporting staff, facilitating a cohesive working environment that allows for direct communication, excellence in service and responsiveness, and direct access to the HPES team by the County for quick resolution of any issues. These sites are:

- Rancho Bernardo. Primary location of HPES staff specifically assigned to support the County. Test environments, training, and video conferencing are housed at this site as well.
- HPES' Tulsa Data Center – Tulsa OK – This is the production data center that will house the majority of the County IT infrastructure, except for that located in San Diego, and delivery of core IT and security services.
- HPES' Colorado Springs Disaster Recovery (DR) site – Colorado Springs CO – This location will be the DR site for the County data center services. It will provide back up or failover capability for all Tier 1 and Tier 2 applications, core services, and data center security services.
- HPES Orlando Data Center – Orlando FL – This location hosts the SIEM services.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Security services for the data center are based on the defense-in-depth model developed by the National Security Agency (NSA). This model emphasizes the use of layers and multiple defense mechanisms across the data center to protect data, systems, networks, and users. In the event that one defensive measure is attacked and exploited, there are more layers and measures behind to continue to protect the assets. This results in real-time threat disruption and time to mitigate or eliminate the consequences of an event. See Section 2.5.4 (Sched 4.3, Section 2.6) for additional information on the defense–in-depth methodology.

The defense-in-depth model also ties to the controls specified in the Risk Management Framework (RMF), which is addressed in Section 2.5.4 (Sched 4.3, Section 2.6). As controls are updated in the RMF roadmap, the defense-in-depth mechanisms and associated delivery processes are reviewed to identify any potential changes. The potential changes will be reviewed with the County to determine implementation approach and timing and are added to the security operations roadmap. This roadmap will contain items to further improve the security posture or maturity of the County from an operational perspective.

All Security hardware and software versions will be evaluated upon release with consideration for feature benefit and risk. Any deviation to standard will be mutually agreed by both HPES and the County. Patches and updates are evaluated as they are made available to determine their applicability to the County environment and will be deployed immediately as needed.

For cloud based solutions, there are two scenarios for security integration:

1. For cloud services hosted by Contractor, Contractor will provide end-to-end security implementation, testing, and continuous monitoring.
2. For cloud services not hosted by Contractor, Contractor will provide, at a minimum, security implementation, testing, and continuous monitoring for all components under Contractor control, such as network and End-User devices.

HPES will follow a detailed Security Management Plan tailored to the County that defines the processes used to provide security services and roles and responsibilities for service delivery. It will describe the technologies and interactions that comprise delivery of security services.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES will use the automated toolsets shown in Table 54. when providing security services to the County.

Table 54. HPES' Automated Security Tools

TOOL	PURPOSE
Symantec Endpoint Protection	Antivirus, antispyware, proactive threat protection (SONAR, application and device controls)
Microsoft Exchange Online Protection	• Antivirus protections • Antispam filters, • Policy enforcement • Graymail detection, safe-unsubscribe • Email based threats (phishing, targeted attacks) • Outbreak filters • Data Loss Prevention • Email Encryption
Palo Alto Next Generation Firewalls with unified threat management capabilities	Firewall services, intrusion prevention services (IPS), spyware and antivirus filtering, web content filtering
Symantec Controlled Compliance Suite (CCS)	Policy compliance for servers
ArcSight SIEM	Security event correlation, log management
Nessus / Tenable Security Center	Vulnerability Scanning
Metasploit	Penetration Testing
HPES Watchdog	Monitors/removes privileged access implemented via non-approved methods (part of the role based access)
Dell Enterprise Reporter	Active Directory Reporting
Dell Recovery Manager AD	Restore deleted or corrupted objects and domain or forest

- Qualifications and Experience – Background and experience in comparable environments

HPES currently performs all required data center security services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: Our Security Operations Center (SOC) gathers feeds from the County's SIEM, firewalls, and IDS/IPS devices for event alerts and notifications, reporting the issues to the County CISO regularly. We manage 16 CheckPoint firewalls; we use HPE TippingPoint IDS/IPS appliances; and manage an ArcSight solution that collects feeds from its firewalls and IPS devices for event logging and threat correlation. Annual penetration testing is performed using Metasploit software. We provide remediation and mitigation including policy pushes for all security devices, security patching, and vulnerability remediation based on security scans.

Department of Housing and Urban Development (HUD): HPES secures all services provided to HUD through our SOC including firewall management, intrusion detection, antivirus management, and computer incident response services. We provide and manage the physical security for our facility. We manage access to the data center so that only authorized staff have access to the facility.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Mainframe Services (Sched. 4.3, Section 6.6)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

With 50+ years of experience managing client mainframes, HPES will ensure a seamless migration to a mid-range environment.

To help the County continue to deliver uninterrupted service to its constituents, HPES will provide seamless, ongoing operational support to the SA16 LPAR Mainframe and A/S400 in Plano until migration to the new, web-based Integrated Property Tax System (IPTS) system. Flawless, predictable support is critical for the timely generation and collection of property tax bills, the major revenue source for the County. Additionally, ongoing support of the Mainframe is critical for accurate and timely delivery of print services for County Tax Statements, in spite of the fact that the Mainframe is operating on obsolete software.

During this time, we will:

- Be responsible for producing and submitting recommendations for standards on production jobs and Job Control Language (JCL)
- Develop and execute plans to retire the Mainframe and A/S400 upon approval from the County.
- Support Mainframe applications for migration
- Measure Mainframe usage in CPU hours and correlate CPU hours directly to end-user processing for specific applications
- Provide hardware and software utilities to support the Mainframe services
- Be responsible for licensing for all hardware and software used to provide Mainframe services.

As long as the mainframe and A/S400 are live in Plano, HPES will support the existing network connectivity that provides end user access, as well as the connectivity to Rancho Bernardo for Managed Print. The DR subscription for the mainframe is provided out of our DR site in Littleton, Massachusetts. Connectivity to Littleton for County End-Users is provided via T1.

Rationale: HPES' first-hand experience with the existing Mainframe and A/S400 environment helps make sure of seamless support and the ability to accomplish the decommissioning activities quickly and efficiently. This experience also facilitates the migration to a mid-range platform for traditional hosted applications without disruption.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The current HPES team, located in Plano will continue to support the Mainframe until migration to IPTS (mid-range) is complete. Additionally, HPES staff located in Rancho Bernardo will continue to support the applications as they do today. Following decommissioning of the mainframe, we will support the IPTS system in Tulsa.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES will use the following four-step process to decommission the SA16 LPAR Mainframe and AS/400 environments.

- Upon completion of the migration to new applications from the Mainframe and AS/400 environments, HPES will decommission the hardware according to standard change management procedures.
- As part of the hardware de-installation process, HPES will perform a complete wipe of the disk and tape storage to remove any County specific data. We will perform a data scrub of all hard drives, permanently removing sensitive data.
- All data stored on tape will be evaluated for archive requirements. If data archive is required, we will convert the tape data for access by the new platform. All other data will be removed (scratched) from the physical media, and either returned to the physical tape scratch pool, or destroyed depending on the condition of the physical media.
- Once the data removal process is complete, we will remove all hardware from WAN and LAN access. The DASD and tape hardware will be returned to the HPES leveraged storage pool for redeployment. The processor environment will be de-installed and securely disposed.

Following the successful decommission of the mainframe and A/S400, all circuit connectivity to Plano and Littleton for the County will be decommissioned, and the DR contract cancelled. Any tape media located at the DR site will be recalled and handled as described in the third bullet above. We will evaluate the connectivity required for the transmission of interface files, and, if necessary, will continue to maintain the dedicated circuit.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES uses more than 150 automated tools to maintain the Mainframe, which come from a variety of vendors including HPE, IBM, and numerous third parties.

- Qualifications and Experience – Background and experience in comparable environments

County of San Diego: HPES designed and continues to support the new UNIX, Wintel, mid-range, and Mainframe architectures that accommodate the platforms and 800+ servers.

HUD – HPES managed a national, agency-wide modernization effort to the mainframe and mid-range server environment, provided an operations help desk and data center environment, and a secure, network environment with complete back-up, recovery, and disaster mitigation support and system controls to monitor network access, system applications, and secure data.

The HUD Information Technology Systems (HUD HITS) infrastructure environment is a complex interdependent set of applications running on many different platforms and running several generations of application design. The largest and most visible application, Computerized Homes Underwriting Management System (CHUMS), has its primary functionality running on a Unisys mainframe.

HPES is supporting more than 250 production applications, which is inclusive of two large mainframes. The IBM mainframe is a 2098 T02 running three partitions and providing in excess of 631 MIPS of processing power.

The IBM mainframe is currently running zOS 1.7, and the HPES HITS team is preparing to migrate the IBM environment to zOS 1.9. The Unisys environment is a Dorado 180 running three partitions and providing 1,000 MIPS. The HPES HITS team is preparing to migrate the Unisys environment to the most current Unisys zOS version (11.3).

Centers for Medicare & Medicaid Services (CMS): Under this contract, HPES has demonstrated its ability to consolidate the mainframe environment, and host a data sensitive, secure environment in support of a multi-tiered customer. HPES has also demonstrated its ability to manage both applications and storage operations (and service desk and website hosting) in the mainframe environment.

HPES provides CMS with a mainframe platform, storage hardware, operating software and 24x7x365 management. HPES' services include hardware planning, installation, and monitoring; hardware and software asset management; hardware and software configuration management; and facilities management in power, cooling, and raised flooring. IT Infrastructure Library (ITIL) client service management best practices are used to make sure that CMS systems meet stringent security policies.

This Enterprise Data Center (EDC) program contract introduces numerous innovations that increased the efficiency of data center operations within the Medicare program, including establishing CMS-managed EDCs, implementing the Internet communications and security architecture, standardizing the process to transition new applications to the EDCs, facilitating tiered pricing, and providing discounts.

HPES successfully transitioned the previous mainframe environment to a HPES managed environment, which is comprised of the following:

- IBM 2097 mainframe that supports CMS, running the z/OS operating system and four logical partitions. We perform capacity and performance measurement reviews monthly, reviewing reports. As of June 2012:
- Tape Library = 1,400 TB virtual tapes
- Total TB of mainframe storage (DASD) = 40TB (raw) and 20TB (usable)
- Hardware – (Mainframe Class B): Z990, 2094/705, 2585 MIPS, 2365 OSA E 1.7 GBIT (2) (Enterprise Extender), DMX2000/3000, MDS-PBI-4, LP10000-E, Sun STK VTS.

HPES successfully migrated mid-tier and mainframe applications to the CMS EDC, on time and to requirements. For mid-tier, this included 16 distributed application/system transitions for CMS and is supporting them in steady-state operations at the VDC. For the mainframe, this included 147 workloads through 47 transition projects.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

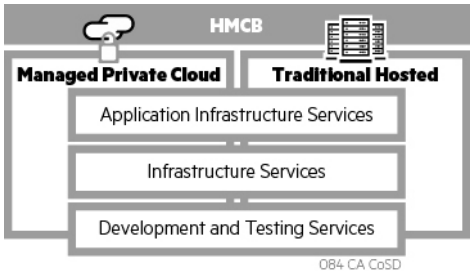
Application Infrastructure Services (Sched. 4.3, Section 6.7)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

To maintain and support County portfolio applications, HPES will deploy hardware and software needed to sustain a hybrid computing solution that crosses three framework services, as illustrated in Figure 105. Our initial implementation will include HPE Helion Managed Cloud Broker solution (HMCB) to provide a high level of automation and orchestration across two pillars: MPC and traditional hosted environments. With HMCB, we have the ability to optimize and manage workloads across MPC, traditional hosted VMware, and, in the future (at the County's discretion), other cloud service providers such as Amazon and Microsoft Azure by providing a full service management solution that gives us a single view of the County's IT assets and governance across service management, financial management, operations, and analytics. By offering a unified approach to managing and deliver high-performance application services, we will reduce complexity and drive consistency, which leads to cost-effective, higher quality services. We recognize that the County is driving for greater levels of virtualization and standardization in the environment, and the MPC will help promote and sustain this objective. For applications that are more complex and require greater customization, the traditional hosted environment enables us to leverage the County's existing technology investments, and reduce risk by maintaining those environments until and unless they are ready to move. Within these two pillars of the design, each framework component has its own resource pools for compute, storage, and network, providing the separation of resources required by the County. This section describes the hybrid environment in general, noting its particular strengths for support of application infrastructure services. The two subsequent sections, Infrastructure Services in response to Exhibit 4.3, Section 6.8) and Dev/Test Services in response to Exhibit 4.3, Section 6.9), do not repeat this material but , please note that all of the same features apply. As previously noted, production applications will not migrate into the MPC during Transition, but will reside in the traditional VMWare environment until refresh, or such time as HPES and the County wish to move them.

HPES will continue to provide application infrastructure services from the Plano and Tulsa data centers. With the planned consolidation to the Tulsa data center, HPES will take this opportunity to move compatible platforms in the current application infrastructure from a traditional hosted environment to a more agile MPC. Application servers eligible to be hosted in the MPC include virtual servers that reside in either the Plano or Tulsa data center today (which will be fully resident in Tulsa following Transition) that fall into a specific range of sizes and will be running current County approved versions of Windows and Linux.

Figure 105. Foundation for Application Infrastructure Services



A common infrastructure provides predictability and higher quality of service for the County.

The pre-defined starting sizes for MPC servers are as follows:

SIZE	CPU ALLOCATION	RAM ALLOCATION
Extra Small	1	2
Small	2	4
Medium	4	8
Large	8	16

SIZE	CPU ALLOCATION	RAM ALLOCATION
Extra Large	8	32

Note that this is only for resource allocation and is unrelated to the billing structure. This range of sizes covers most of the servers in the environment that have a compatible operating system. For servers whose resource requirements are higher (e.g., servers that require 64GB or more of RAM), they can still be deployed in MPC as Extra Large, then the resources can be scaled up to meet the application's requirement. As of the time of the analysis for this proposal, fewer than 10 servers in the environment fell into this category; hence, we did not design additional sizes. If, however, larger resource requirements become more prevalent, additional sizes can be added.

Table 55 illustrates the possible distribution of the server environment, by application, between Traditional and MPC. Note that Traditional includes Mainframe, AS400, Solaris, HP-UX, AIX, and Appliances (custom hardware) as well as servers that currently reside outside of Plano or Tulsa but within the scope of Data Center Services. This list is a snapshot in time as of when the original analysis was performed for the proposal. At the start of Transition, it will be updated to reflect changes in the environment.

Table 55. Hosting Strategy by Application

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
Column 1 – App has Servers Eligible for MPC | Column 2 – App has Dev/Test Servers Targeted to be Persistent in MPC | Column 3 – App has Environments Targeted for Traditional Hosting				
PA1002	AIS Master Mailing List	Y		Y
PA1005	AAB Labels			Y
PA1008	ACAP/ACVV Values, Rates, Apportion			Y
PA1014	Accounts Receivable and Trust			Y
PA1017	ACRC Roll Corrections Process	Y		Y
PA1018	ACST/TC Auditor Secured Tax Billing			Y
PA1019	ACTI Tax Rate Area Index			Y
PA1020	ACUS Auditor Unsecured Prpty Tax Billing			Y
PA1024	Agricultural Preserves	Y		
PA1044	ASAD Secured Prpty Assess Info System			Y
PA1045	ASAS Secured Prpty Assess Ownership&Valu			Y
PA1046	ASPA Supplemental Property System			Y
PA1047	ASRC Roll Corrections Process	Y		Y
PA1048	Assessment Appeals Board System	Y		Y
PA1049	ARCC Intranet Applications	Y		
PA1050	ARCC Internet Applications	Y		
PA1054	Audit Assignment Tracking	Y		Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA1058	AutoCAD			Y
PA1073	CDS Online	Y		Y
PA1074	CDS Batch	Y		Y
PA1077	Ballot Enclosure Scanning System			Y
PA1136	Chameleon	Y	Y	
PA1158	Community Enhancement / Neighborhood Reinvestment Program (AC Grant)	Y	Y	Y
PA1159	iVOS	Y		Y
PA1160	Comparable Sales System			Y
PA1162	Computer Assisted Mass Appraisal (CAMA)			Y
PA1174	County Law			Y
PA1179	Criminal Case Tracking-JURIS			Y
PA1187	Cut Log Tracking			Y
PA1188	County Intranet Site	Y		
PA1196	CME Web	Y		Y
PA1202	DHR Internet Class/Comp info.			Y
PA1247	Field Survey Notes Index	Y		
PA1270	Geo-Coding System			Y
PA1308	TTC Sonant IVR, ACD and Phone Payment System	Y		Y
PA1310	Homeowner Exemptions - AS/400			Y
PA1313	IBM - Probation Records			Y
PA1314	IDX Managed Care Application	Y	Y	Y
PA1324	Interest Apportionment			Y
PA1376	Traffic/Minor Offense Mainframe			Y
PA1389	MPR Online			Y
PA1409	Officer Notification System			Y
PA1433	PAR File Online			Y
PA1438	Precinct Activity Tracking System			Y
PA1451	Performance Reports	Y		
PA1516	Prop 60/90/110	Y		
PA1517	Prop 8	Y		Y
PA1523	TTC Tax Sale Database	Y		

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA1564	Records Index			Y
PA1566	Redemption (Prior Year/Secured/Defaulted) Taxes			Y
PA1568	DPW Referrals System	Y		
PA1580	Restraining Order System			Y
PA1588	RSVP Volunteer Reporter	Y	Y	Y
PA1595	Sale of Data			Y
PA1603	Section 11 Properties	Y		
PA1609	Sheriff ID			Y
PA1610	Sheriff Licensing			Y
PA1611	Sheriff Registrants			Y
PA1643	Supplemental Online			Y
PA1659	Timeshare Ownership Tracking	Y		Y
PA1665	Criminal History Tracking System			Y
PA1680	TTC TRDS Defaulted Secured Data Mgmt (Mainframe)	Y		Y
PA1682	TTC TRST Tax Collector Secured Tax Collect (Mainframe)			Y
PA1683	TTC TRTC Carryover (Mainframe)			Y
PA1684	TTC TRTH Secured Tax History Info System (Mainframe)			Y
PA1742	TTC TRRT Unsecured Tax Refund Mgmt System (Mainframe)			Y
PA1745	TTC TRUS Unsecured Property Tax System (Mainframe)			Y
PA1755	Volunteer Tracking System Polinsky	Y		
PA1759	Want/Warrant System	Y		Y
PA1766	Weather Monitoring and Flood Warning System	Y	Y	Y
PA1782	Adoptions Assistance Program			Y
PA1785	Animal Control - Lost and Found	Y		
PA1788	Autocad	Y		
PA1789	AutoLISP Files	Y		
PA1802	TTC TRCC Cortac (Mainframe)			Y
PA1809	CWS/CMS Data Mart			Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA1813	TTC Tax Sale Maps and Images (Web)	Y		Y
PA1814	DHR Internet Web Page			Y
PA1820	EMISSIONS INVENTORY (EASIER)	Y		Y
PA1846	Natality Extract for Dr. Dobkins, UCSD	Y		Y
PA1855	Phone Directory (INTRANET)	Y		
PA1856	Precinct District Voter Counts			Y
PA1857	Preliminary Notices	Y		
PA1865	Property Tax Characteristics	Y		
PA1869	Rasscle			Y
PA1871	Recorder Vital Records System	Y		Y
PA1872	Red Envelope			Y
PA1887	SIMWIN			Y
PA1893	Tax Rate by Tax Rate Area Search	Y		Y
PA1900	Tran Control Log: Shrink Wrap	Y		
PA1901	Traverse	Y		
PA1902	ARCCs AX/WX/WFM Applications	Y		Y
PA1905	Web Polling Place Lookup	Y		Y
PA1907	Kinnosa	Y		
PA1917	Chargeback System	Y		
PA1920	Sales/Deposit Permit System	Y		
PA1921	SSRS			Y
PA1922	Training Tracking	Y		
PA1923	Countywide Customer Satisfaction Survey			Y
PA1927	Polinsky Donor Tracking System			Y
PA1928	EZ Access			Y
PA1933	ARCC E-Commerce	Y		
PA1940	CMIPS Adhoc Tool	Y	Y	Y
PA1971	SUN (San Diego User Network)			Y
PA1973	ISCP - CODE 1 Plus			Y
PA1974	ISFC - FOCUS Front-End Processing			Y
PA1976	ISTB - Telephone Billing			Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2005	County Web Mapping Applications	Y		
PA2012	Q-Matic Line Queue Management	Y	Y	
PA2031	Juvenile Traffic			Y
PA2044	Public Defender Intranet (PD)	Y		
PA2056	Edgemore Nurse Staffing program			Y
PA2057	EZ Access Interfacing Systems			Y
PA2060	PeopleSoft HCM	Y	Y	Y
PA2065	Polinsky Kids Information Data System	Y	Y	Y
PA2068	Administrative Investigations Management	Y		Y
PA2078	TTC Mobile Home Tax Clearance Database	Y		
PA2079	Parent/Child Property Transfer System	Y		
PA2081	Property Parcel Corrections Database	Y		
PA2082	ARCC Document Management System	Y	Y	Y
PA2083	Certificate Signature Printing System	Y		
PA2089	Marshall-Swift Commercial/Agricultural Estimator	Y		Y
PA2090	MLS	Y		
PA2093	Integrated Report Systems (I.R.S.)	Y		
PA2094	Outside Purchase Control System (OPTICS)	Y		
PA2100	EZ Access - Jwalk			Y
PA2102	Jail Information Management System Interfaces			Y
PA2103	JCATS Criminal Case Management System		Y	Y
PA2110	Vital Records Information System	Y	Y	Y
PA2113	Public Health Information System	Y	Y	Y
PA2115	Banknote Paper Tracking	Y		
PA2127	Prof Photocopiers	Y		
PA2134	Survey Records Imaging System	Y	Y	Y
PA2135	HR Employment Document Management System	Y	Y	Y
PA2144	SPS Cut	Y		
PA2150	ERP Oracle Financials	Y		Y
PA2152	Business Audit Tracking	Y		
PA2153	Fraud Referral Tracking System	Y	Y	

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2154	Secure Web Drop Box	Y		
PA2156	Bar Code File Tracking System			Y
PA2171	NTTData Netsolutions	Y	Y	
PA2175	SOCAT			Y
PA2186	Elite	Y		Y
PA2190	SPSS	Y		
PA2191	QANET Collector System	Y		Y
PA2193	TTC ApplicationXtender & WebXtender	Y		
PA2200	Child Health and Disability Program/Children Youth and Families/Health Care Program for Children in Foster Care	Y	Y	
PA2201	TTC Wausau ImageRPS	Y		Y
PA2202	Sharpe IPM	Y		Y
PA2210	Workflow Manager for Revenue and Recovery Remittance System	Y		
PA2211	ERMXtender for ARCC	Y	Y	
PA2215	Utility Manager Pro	Y		
PA2224	Volunteer Tracking System AIS	Y	Y	
PA2233	DIMSNET	Y		Y
PA2235	Probation Case Management System	Y	Y	Y
PA2237	ARCC Cashiering	Y		Y
PA2238	Innovative Millennium	Y		Y
PA2239	Special Assessments by Parcel Number Search	Y		Y
PA2242	Buynet II	Y		Y
PA2245	Kronos Workforce Central	Y	Y	Y
PA2250	AXAddOns	Y		
PA2257	Source Test Tracking			Y
PA2260	Hansen for Parks & Rec	Y		
PA2261	QBIS Data Recording System (DRS)	Y		Y
PA2262	San Diego Immunization Registry	Y	Y	Y
PA2263	OneStep Database	Y		
PA2264	Mystery Shopper			Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2265	HHSA Program Guides	Y	Y	Y
PA2267	WebTrends	Y		
PA2270	External Agencies WEB Reporting	Y		Y
PA2273	LUEG Repository	Y	Y	Y
PA2286	TTC Trustref (TTC Financial Apps)	Y		
PA2287	Viking Data Entry System	Y		
PA2288	ARCC Recording System	Y		Y
PA2289	ARCC Mills Act DB	Y		
PA2293	Manual Clearing Database	Y		
PA2295	Purchasing and Contracting Documentum Repository	Y	Y	Y
PA2300	TTC WARP (Wire Access Request Portal)	Y		Y
PA2308	PHIX	Y	Y	
PA2309	AutoCAD Raster Design	Y		
PA2313	Columbia Ultimate RPCS	Y	Y	Y
PA2314	Grant or Community Enhancement	Y	Y	Y
PA2315	Medical Therapy Unit Online	Y	Y	
PA2318	ROP Mobile Home DB	Y		
PA2319	Rental Mobile Home DB	Y	Y	Y
PA2324	Kofax Ascent Capture 7.0			Y
PA2337	Case Review System	Y	Y	
PA2340	SDE Repository	Y		
PA2341	File Tracking System	Y	Y	
PA2343	Closed Cases Repayment Accting System	Y	Y	Y
PA2344	Cal Win Interfaces	Y		Y
PA2351	BOS District One Website	Y		
PA2352	BOS District Two Website	Y		
PA2353	BOS District Three Website	Y		
PA2354	BOS District Four Website	Y		
PA2355	BOS District Five Website	Y		
PA2356	Applications Manager	Y		
PA2357	Accela Automation (BCMS) (LEAMS)	Y	Y	Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2358	COB Public Search	Y	Y	Y
PA2360	PCC Staffing Database			Y
PA2361	myRequests	Y		Y
PA2369	Parent Search db			Y
PA2371	Case Folder Tracking			Y
PA2378	WITS	Y		
PA2385	CMS Patient Eligibility System	Y	Y	Y
PA2391	MaxCars	Y		
PA2397	PatternStream	Y		Y
PA2399	Property Profile Mapping	Y		
PA2407	Food Facility Inspection Search	Y		Y
PA2413	County Web Referrals	Y	Y	
PA2415	CCS Web Referrals	Y	Y	
PA2417	CalWIN CIS Data Mart	Y		Y
PA2422	Proscript	Y	Y	Y
PA2427	Absentee Voter Lookup	Y		Y
PA2429	ArborPro Management System	Y		
PA2430	NeoGov	Y		Y
PA2432	Northpointe COMPAS	Y		
PA2434	Kofax Ascent Capture - FG	Y		Y
PA2438	TTC WITS (Web Integrated Tax System)	Y		
PA2439	APS Imaging	Y	Y	Y
PA2444	Citizen Advisory Boards Application	Y	Y	Y
PA2445	Cerner Millennium	Y	Y	Y
PA2446	Pharmacy Outpatient System (Etreby)	Y	Y	
PA2447	Budget Books	Y	Y	Y
PA2449	QCS AdHoc Statistical Reporting Subsystem			Y
PA2455	HR Documentum	Y	Y	Y
PA2456	CWS Mandated Reporter	Y	Y	
PA2458	Prodagio	Y	Y	Y
PA2459	ERP Data Archive	Y		

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2461	TTC CRS (Central Reporting System)	Y		
PA2462	Card Access System			Y
PA2468	AIS Ombudsman	Y	Y	Y
PA2469	AIS Case Management	Y	Y	Y
PA2470	StarLIMS - Web	Y	Y	Y
PA2471	BMC Footprints	Y	Y	Y
PA2477	TB - Fujifilm	Y		Y
PA2478	TTC Bloomberg Gateway	Y		
PA2479	HHSA HR Kofax Imaging	Y	Y	Y
PA2480	HHSA AIS Ombudsman Kofax Imaging	Y	Y	Y
PA2481	HHSA AIS APS Kofax Imaging	Y	Y	Y
PA2482	HHSA AIS Case Management Kofax Imaging	Y	Y	Y
PA2483	ARCC Q-MATIC Orchestra	Y		
PA2484	ARCC Captiva Scanning Solution	Y		
PA2485	AIS-IHSS Kofax Imaging	Y	Y	Y
PA2486	AIS - IHSS Documentum/Webtop	Y	Y	Y
PA2489	iQCS	Y	Y	Y
PA2490	Electronic Approval Workflow	Y	Y	Y
PA2491	CATS Customer Dashboard	Y		
PA2492	CRM Framework	Y	Y	
PA2493	Integrated Recording & Vital Records System (aka. ACCLAIM)	Y		Y
PA2494	Medical Standards In-service Tracking	Y		
PA2495	AtPac Asset Manager	Y		
PA2496	Convey 1099	Y	Y	
PA2499	TTC iPayment Cashiering	Y		
PA2501	DCSS Data Warehouse	Y		
PA2505	Inventory and Resource Management System	Y		
PA2507	Actuate BIRT 11	Y		Y
PA2509	ERP Oracle Data Warehouse	Y		Y
PA2510	PA Enrollment			Y
PA2511	DGS Generic Filing Cabinet	Y	Y	Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2512	Public Authority Payroll History	Y	Y	Y
PA2514	Documentum Import Tool	Y	Y	Y
PA2515	PARTS - Public Authority Registry Tracking System	Y	Y	
PA2518	Oracle Identity Manager	Y		
PA2519	ALEX (not an acronym)	Y	Y	
PA2520	CalWin Case Comments	Y	Y	
PA2524	Performance Budgeting	Y		Y
PA2525	AuditExchange	Y		
PA2527	TTC SharePoint iTTC	Y		
PA2530	ApprMapr - Web mapping application	Y		Y
PA2532	Justice Electronic Library System	Y		
PA2533	Community Resource Directory	Y		
PA2534	Oracle Fusion Middleware			Y
PA2535	TTC Ad-Hoc Bill Printing			Y
PA2536	Care Transitions Coach System			Y
PA2538	Public Defender eShare	Y		
PA2540	Documentum Records Manager	Y	Y	Y
PA2541	Building Automation System	Y		
PA2542	ARCC SharePoint Site	Y		
PA2543	P-Card Access Database			Y
PA2544	PCMS To HHSA Interface	Y		Y
PA2546	County Constituent Relationship Management	Y	Y	Y
PA2548	CobbleStone Data Synchronization			Y
PA2549	IPTS-GRM	Y		Y
PA2557	Crossroads Software Collision Database System	Y		
PA2558	Identity and Access Management	Y	Y	Y
PA2561	Cerner CareTracker	Y	Y	
PA2562	CalWIN ERMS	Y	Y	Y
PA2563	Enterprise Document Processing Platform	Y	Y	Y
PA2567	San Diego Regional Resiliency Checkup	Y		
PA2569	ROV Documentum Generic File Cabinet	Y	Y	Y

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2571	Nicus M-PWR	Y		
PA2572	Client Visit Management	Y	Y	
PA2573	Web Application for Legacy Payroll Data and Reports	Y		
PA2574	Pyxis	Y		Y
PA2575	Beach and Water Quality (BWQ)	Y		Y
PA2576	DCSS Business Intelligence - Tableau	Y		
PA2578	County Internet Website (AEM)	Y		
PA2580	LAFCO ApplicationXtender (AX) Imaging Environment	Y		Y
PA2581	TTC Interactive Web Response (IWR)	Y		
PA2582	GIS Mobile Applications			Y
PA2583	CAR			Y
PA2584	AP Invoice Imaging System	Y	Y	Y
PA2586	Enterprise Email Solution			Y
PA2587	A&C Captiva Scanning	Y	Y	Y
PA2588	PCMS Knowledge Center	Y		
PA2589	PCMS Biometrics	Y		
PA2590	DocVault	Y	Y	Y
PA2592	TempTrak	Y		
PA2593	DHR Document Repository for Medical Standards	Y	Y	Y
PA2594	Probation Electronic Medical Records System (PEMR)	Y		
PA2595	Granicus - Citizen Participation Suite			Y
PA2597	SharePoint 2013 Platform	Y		
PA2598	LiveWellSD.org	Y		
PA2599	Adobe e-Forms DEH Inspections	Y	Y	Y
PA2600	TTC SeeTrans	Y		
PA2601	TTC EPS Express Manager	Y		
PA2602	EPI HIE SFTP Access	Y		Y
PA2603	DHR Captiva7 Scanning	Y		
PA2604	Probation Contact Log Mobile Application (PUMA)	Y		

PAID	NAME	COLUMN 1	COLUMN 2	COLUMN 3
PA2605	Transform for CalWIN Checks/Warrants	Y		
PA2606	DHR Documents upload to Documentum	Y	Y	Y
PA2607	Bad Check Database			Y
PA2608	Balance Due Report DB			Y
PA2609	eForms Repository	Y	Y	Y
PA2611	CoSign Digital Signature	Y		Y
PA2613	TTC AEM Internet Site (SDTREASTAX.COM)	Y		
PA2614	Information Exchange Program (ConnectWellSD)	Y	Y	Y
PA2615	ROV AEM Website (SDVOTE.COM)	Y		
PA2617	Probation Work Projects	Y		
PA2618	DHR BENEFITS ELECTRONIC DOCUMENTS UPLOAD	Y	Y	Y
PA2619	Selectron IVR			Y
PA2620	Facil			Y
PA2621	Alzheimer's Project AEM Website (SDAlzheimersProject.org)	Y		
PA2622	SDPARKS AEM Website (www.sdparks.org)	Y		
PA2629	Adobe e-Forms APCD Inspections	Y	Y	Y

The hybrid environment can support application infrastructure services, infrastructure services and Dev/Test services (for both Applications M&O and Development and Test projects). The MPC and the traditional hosted infrastructure are sized to accommodate the combined workloads from Plano and Tulsa, and can scale as needed to support the County's needs. Since, at the time of this submission, all of the County's VMWare environments are compatible with the basic cloud requirements, the approximate split of servers between the Traditional and MPC environments is as follows:

Development (Dev/Test + M&O)	271	60
Production	448	181

In support of the County's Virtual First strategy, we will continue to pursue virtualization of as much of the remaining physical environment as possible. When each server comes up for refresh, we will analyze the rationale for keeping it on a physical server vs migrating to a virtual (and, if possible, migrating it into the cloud environment), and if there is no technical reason a physical server is required, we will redeploy the server's applications into a virtual server and dispose of the vacated hardware.

Resource Unit Management Post-Transition

As new applications are developed that are targeted to run in the MPC, the HPES team will request MPC resources through the provisioning interface, including servers, software, storage, and backup requirements. Once the demand request is received by the system, and the automated parts of the provisioning process complete, the Applications team will then be responsible for installing, configuring, and testing each application component.

Conversely, as applications are retired or their Dev/Test components are no longer needed for live use, and therefore the associated MPC resources are no longer needed, the Applications team will submit a service request to de-install the MPC infrastructure for that application. The team will decommission all of the application components and infrastructure resources for the application environment being retired, and release any licenses through Asset and Configuration Management. If the environment is a dev/test environment, the request will specify whether the environment should be permanently decommissioned or put into cold storage. If the latter applies, the image will be preserved on the storage area network (SAN) storage and held in an online inventory, but its compute resources released. Otherwise, all resources will be released.

From a RU billing perspective, RUs are added to billing at the point a production server environment is made available for County use. RUs are removed from billing at the point when a request to decommission a production environment is issued and approved. If a production application moves from a traditional hosted environment to MPC post-Transition, there is no change to billing. During Transition, the County will not be billed for both sets of RUs for any given server.

After Transition is complete, moves between the traditional Dev/Test environment and MPC hosted Dev/Test environment will not have an impact on billing. Changes to the overall scope of the Development & Test Environment RU will follow the contract change control process.

For additions to the Dev/Test environment, if the application resource requirements are large, such that its requirements exceed the capacity available (this scenario will be the exception rather than the rule), HPES may need to acquire more resources and modify Resource Unit fee accordingly. In most cases, the resources will be available, and the environments will be added with no change to RU billing. By the same token, removal of applications from the Dev/Test pool will not trigger a change to RU billing.

For a description of how we will manage RU billing during Transition, please refer to Section 2.11, Transition Services.

Managed Private Cloud Specifications

The HPE Helion Managed Private Cloud solution is built on a predefined, dedicated solution that enables us to rapidly deploy server, storage, and network infrastructure "as service" for the County via a secure, web-based Private Cloud Portal.

The comprehensive private cloud solution includes HPE hardware and software, professional consulting and implementation services, and ongoing end-to-end management services. The foundation for the solution is HPE CloudSystem Foundation, the market's most complete, integrated, and open cloud platform. HPE CloudSystem Foundation is a pre-integrated solution that will enable HPES to create and manage virtual pools of servers, storage, backup, and networking resources on behalf of the County using a common management layer.

Helion MPC solutions leverage CloudSystem Foundation to provide a predefined, prebuilt, highly standardized infrastructure environment that leverages a building block approach. The configurable

infrastructure environment consists of a set of preconfigured, dedicated hardware building blocks for computing, storage, backup, and connectivity. These building blocks—which can be scaled independently—serve as the underlying, enabling infrastructure used to provide the standard Infrastructure-as-a-Service (IaaS). There is a base service to which optional services, or building blocks, can be added. Using this approach, we have designed an MPC solution that is configured to the County requirements, including selection of the mix of virtual machine (VM) sizes and operating system distribution that best map to the County's application profile.

Standard hardware-related services supporting the private cloud environment include but are not limited to the following:

- Hardware installation and configuration
- Hardware management
- Capacity management
- Problem monitoring, including proactive hardware support
- Release management
- Patch and system driver management
- Data center facility (floor space, power supply, cooling, wiring)
- Installation of management software

Some of the standard hardware and software products are as follows:

- **Server, Storage, and Backup Devices** – MPC uses HPE's Converged Infrastructure including ProLiant Gen9 blades running inside c7000 blade enclosures. Integration with SAN-based storage and backup devices is required in support of an MPC environment. Our private cloud offering uses 3PAR storage options as a configuration standard.
- **Cloud Service Automation (CSA)** – Combined with Operations Orchestration (OO), CSA automatically enables the design and provisioning of infrastructure services in minutes along the user-requested infrastructure configuration. HPE Server Automation software enables us to automatically perform activities such as server discovery to provisioning, patching, configuration management, and script execution to comply with HPES and County IT configuration standards. CSA also provides the foundation for the cloud service catalog presentation, automation, management, and orchestration.

With MPC, HPES provides an advanced level of skilled operations and engineering talent who manage and monitor the cloud environment. This team manages the server, storage, backup, and networking resource pools along with System Management Software, such as HPE Server Automation software layers. These products help to facilitate the day-to-day operational support for the converged infrastructure-based cloud resource pool. They automatically deploy predefined Windows and Linux operating systems into the environment via predefined workflows.

We deploy monitoring, antivirus, and policy compliance agents as part of the automated workflows. The consistent and reusable private cloud infrastructure will enable the County to rapidly access the infrastructure when needed. We maintain and manage all the software, agents, and monitoring infrastructure of the private cloud.

We support other key components of the private cloud computing environment, such as CSA and the Private Cloud Portal. We support Operations Orchestration, managing the CSA Database, Cloud Controller, and CSA Provider Console, including the following activities:

- Administering the standard Service Request Catalog
- Managing specific CSA settings
- Responding to subscription requests
- Providing lifecycle management of catalog operations

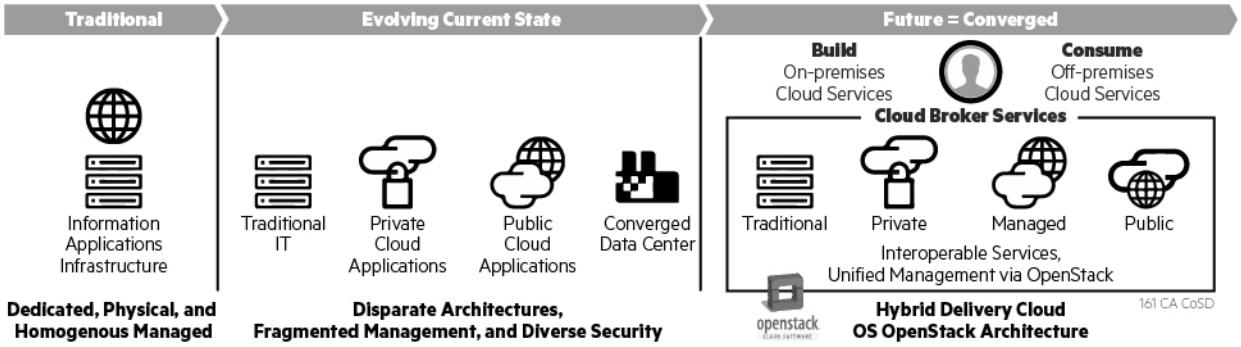
- Supplying standard consumption reports

Implementation of the HPE HMCB will further streamline the management and operations of the County's hybrid environment. It will help us achieve an integrated view of the County's hybrid IT ecosystem and provide the ability to manage VMware-based virtual workloads in the traditional hosted environment both inside and outside of the data center.

HMCB is designed to mitigate the challenges of procure, deploy and service management through a unified approach to handling provisioning, IT spend and performance, workload placement, and security and compliance requirements. As a result, hybrid-provided services can be governed and modeled across service management, financial management, and operations. For example, the governance aspect helps the County identify how efficiently their money is being spent by recognizing usage patterns and capacity used. In the future, when the County is ready and through HMCB, HPES will provision, manage, and report on County services hosted in public clouds, such as Microsoft Azure and Amazon Web Services (AWS), providing a consolidated view of the entire environment.

With implementation of a hybrid environment in the Tulsa data center, we will bring application infrastructure improvements throughout the life cycle of an application, whether it is in the MPC or the traditional environment, and whether it resides on a physical server or a virtual host. To improve physical provisioning time, for typical orders of a few servers, HPES will keep spares on hand so that for standard configurations there will be no wait for procurement. We will continue to identify opportunities to automate workflows to further improve provisioning of traditional environments to meet or exceed the County's service level requirements. Our complete pre-integrated hybrid cloud solution will bring to bear data center-wide streamlined service creation, deployment, and monitoring for application workloads, as illustrated in Figure 106. .

Figure 106. HPES MPC Standard Building Block and Scale Out Approach to MPC Resources



Implementation of this this approach will streamline service deployment and easily grow or contract application infrastructure resources.

HPES data center services are presently in an evolving current state, today, we have a mix of:

- Traditional IT (multiple server platforms and mainframe)
- A few servers in the HPES Government community cloud (also known as the Helion Virtual Private Cloud)
- Software as a Service (SaaS) applications hosted by third-party providers
- A few Infrastructure as a Service (IaaS) instances in the Microsoft Azure public cloud.

In the new solution, we will implement the hybrid delivery architecture shown above under the rightmost arrow ("Future = converged") to bring these disparate silos together. For the remainder of this framework response, we will focus primarily on the MPC and traditional environments, since this is where most of the County's critical workload and requirements are concentrated today. However, we recognize that the

VPC, SaaS, and public IaaS environments will continue to be a part of the County's hybrid delivery services. Once in place, our Cloud Broker will form the basis to create a continual improvement plan and roadmap. This plan will unify and bring transparency and consistency of governance to these environments, and we will help the County target future workloads for the right provider and delivery model.

Our hybrid solution will provide the following benefits to the County:

- **Faster time to value**. Using the MPC, we will provide a standard content library with approved County template virtual server (VMs) images that can be provisioned in a matter of hours rather than weeks or months. The standard templates will allow application solution teams to quickly request web, application and database VMs with preapproved and configured images for the County landscape helping drive the County's "virtual first" strategy.
- **The right hosting solution for any application**. For applications that require a high level of customization, such as use of non-standard platforms, our traditional hosting service provides this solution.
- **High performance application services:** This will result in better service to End-Users, third parties and constituents of the services.
- **HMCB:** Consolidated management and financial governance of traditional, private, and public cloud hosted environments.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES will continue to provide application infrastructure services for the County applications portfolio in our Tulsa and Plano data centers, until the consolidation to the Tulsa data center is complete, approximately nine months after contract award. We will migrate all workloads from Plano to Tulsa as described Section 2.11 (Schedule 2.1, Section 3.4) of this proposal.

Within these environments in Tulsa, the HPES team, which includes your local team in San Diego, our service center in Pontiac Michigan, and our virtual teams of subject matter experts (SMEs), situated throughout the United States, will continue to manage and operate the application infrastructure services required by these applications.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES uses a life cycle approach to support applications infrastructure. It begins with planning to add or change applications and identifying application infrastructure requirements, recognizing that not all County applications are or will be compatible with MPC. Although this is our preference, we will follow an application placement methodology in which we assess cloud readiness. We will look at each County application in the production inventory and analyze where that application would best be deployed based on evaluation of the following types of requirements:

- Regulatory requirements
- Performance requirements
- Adherence to infrastructure standards
- Security and confidentiality
- Availability and reliability

When designing the infrastructure to support an application, we determine which tiers are required. The tiers will include the presentation layer, business logic (application) layer, and the back-end (database/transaction) layer. The infrastructure to support any tier can be either MPC or traditional. The

County's network zones are supported transparently in both environments. The zones are described in the Security Services section (Schedule 4.3 Section 6.5).

Prior to migration, we will build out the MPC and upgrade and expand Tulsa's traditional environment to include the required infrastructure for servers, storage and networking components to accommodate the migration of applications into this facility. As part of the consolidation, we will analyze the current application environment and identify the candidate environments to move into the MPC. When this is complete, candidates from the Tulsa environment will be moved into the MPC to further consolidate and standardize workloads. Upon refresh and subject to County-defined limitations for periodic refresh cycles, we will continually evaluate additional application workloads to assess the feasibility of moving these to the MPC. We will analyze items such as County investment, timeframe for application retirement, if any, and the complexity of the development effort for legacy applications to be re-architected in MPC.

As required today, for all application infrastructure upgrades, refreshes, and transformational activities that impact portfolio applications, HPES will continue to update and maintain AppsManager with information needed in eRunbooks. Application infrastructure examples will be updated DNS, system patches, and sections for outage and notifications, data center and escalation contacts, application interfaces, AD/service accounts and document links, whether provided in the MPC, traditional hosted, or other cloud environments.

Performance Analysis and Improvement

We use a variety of methods to analyze performance (and capacity, because these disciplines are often related) of data center assets, as illustrated in Figure 107.

Figure 107. Performance Management Approaches

Approaching Performance and Capacity Management from all possible angles drives continuous improvement.

Reactive Performance Management comes from responding to the early warning alerts we get from our tools—they automatically contact us to look into a situation where some resource or performance metric has passed a threshold point. By reacting to these warnings in a timely manner, we can often prevent issues caused by surge spikes or rapid increase in consumption of resources.

Of course, the worst case is when we have to respond to an incident for system slowdown. If this happens, as part of our root cause analysis we examine the configuration of our early warning systems to determine whether new thresholds need to be added or if existing ones need to be made more sensitive to detect problems before they become apparent to users.

Proactive Performance Management involves reviewing the trend analytics and reports on capacity and performance—we review the performance and utilization (capacity) trends on our systems on a daily basis. This helps us spot indications that activity or consumption is increasing,

From a pure capacity management perspective, this process also helps us identify underutilized resources that can be targeted for downsizing, consolidation, or shutdown. We will review the results of these analyses with the County and make recommendations for County approval.

Focused reviews are point-level reviews. Typically, if we are getting ready to embark on a project such as a major change or upgrade to an application, we would review the infrastructure's performance and capacity characteristics to determine whether changes need to be made to accommodate the needs of the project.

Performance improvements, in response to either reactive or proactive scenarios, include tuning configuration parameters, adding capacity, or making an architecture change such as re-shaping network traffic or moving data to a different storage tier.

HPES also follows the same methodologies and processes to manage the application infrastructure as we do for infrastructure services, which is described in the next section, in response to Schedule 4.3, Section 6.8.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES automated tools to provision and de-provision capacity for MPC and traditional environments are detailed in Table 56. These tools help us respond quickly to changing requirements from the County to optimize the applications infrastructure and to reduce cost by decommissioning unnecessary services:

Table 56. HPES' Automated Provisioning Tools for Managed Private Cloud

TOOLS	FUNCTION
HPE Cloud Service Automation	Automation of cloud management and provisioning
Helion Managed Cloud Broker	This tool is extendable to remote virtual environments and can integrate with public cloud vendors such as Amazon Web Services and Microsoft Azure
HPE Server Automation	Software patching and software distribution
HPE Operations Orchestration Server (OO)	Process workflow automation
Operations Orchestration Remote Access Server	Remote access to OO
HPE Operations Manager	Cloud infrastructure monitoring
VMware v-Center	Server virtualization management
Veritas Infoscale or Symantec Storage Foundation	Filesystem management and clustering in specific Solaris environments

For application infrastructure we also use HPE SiteScope for monitoring application thresholds and events. Network and storage/backup systems and tools are described in Section 2.8 of this proposal (in response to Schedule 4.3), Section 5 and Section 2.9 (in response to Schedule 4.3 Sections 6.12/6/13 respectively).

The operating system and database management software of the various platforms contain numerous tools and facilities used to configure, manage, monitor, and provide high availability to particular environments. These are not listed here. Security tools applied to the application infrastructure environment are described in response to Schedule 4.3 Section 6.5. Tools for storage services are described in response to Schedule 4.3 Section 6.12.

- Qualifications and Experience – Background and experience in comparable environments

HPES currently performs all required application infrastructure services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: We monitor the health of more than 400 steady-state business applications and assist in troubleshooting infrastructure issues. We provide system, application and Oracle and SQL server database support for the County's applications. Our dedicated staff supports the County 24x7x365.

HUD: HPES hosts more than 200 applications, providing more than 450 terabytes (TB) of data storage, DR for 35 applications, and wireless services to more than 1,600 mobile devices. At contract start, we acquired a data center facility that was fully ready to support HUD needs in Charleston, West Virginia. We planned, engineered, coordinated, and executed a flawless transition of HUD's production applications and their development and test environments seamlessly and without interruption. We completed a complex, 6-month transition project on time, under budget. We met or exceeded 97% of service levels. Following weeks of planning, we seamlessly migrated more than 200 applications to our data center without disrupting HUD's operations.

U.S. Navy Marine Corps Intranet (NMCI): HPES established a centrally managed, secure application hosting environment to support enterprise applications. Our managed hosting support includes solution development, migration/engineering assessment, service preparation and setup, facilities and inventory, server management, client services, database management, application administration, storage management, applications hosting network hosting services, information security services, and DR. We manage 4,400 enterprise-wide servers and 1,183 virtualized servers running at 27 different virtualized sites. We operate and maintain the Next Generation Enterprise Network (NGEN) classified and unclassified storage capabilities including software, hardware, processes, and tools to facilitate the management and reporting of different classes of storage services across a wide range of workloads and applications.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

The MPC and HMCB solutions included in the Transition for the County include support for all of the functionality required by the County today. The MPC offering today has other capabilities that were considered but not chosen for deployment in the County environment – either because

(a) they were not specifically required to meet current and expected needs;

(b) an alternate solution was chosen for that particular function (generally because it could meet the needs of both the traditional and MPC environment without having to have two separate solutions), or

(c) we know these functions are currently not desired by the County.

We offer this list for completeness and for future consideration, so that, as the County's cloud requirements evolve, they can be reconsidered.

- Portal for self-service ordering and provisioning

- Two Factor Authentication
- Hyperconverged Infrastructure
- TippingPoint solution
- App Detective solution
- HMCB Analytics module
- Automated provisioning of physical servers

The CSA and OO components that drive the automation for MPC and HMCB are almost infinitely customizable. The HPES portfolio team provides regular releases of both offerings that will be evaluated and tested for applicability and value to meet the County's objectives, as they are released. We also offer two optional RUs to expand the service, if and when the County chooses to use them. These would be expansions to the solution rather than alternatives to it:

- Ability to provision into and monitor/manage virtual servers in public clouds, such as Amazon Web Services and Microsoft Azure (this capability is available without customization, but is an add-on to the core service).

To demonstrate the flexibility and customization ability of the HMCB solution, we have included an optional RU to enable the Broker to provision into the Oracle VM Server for SPARC platform as an alternative to leaving this platform in the traditional hosting environment. Because the County does not have a significant footprint using this platform at present, our viewpoint is that ordering this RU would add limited value until the volume of virtual servers reaches 100 or more. Some additional capabilities we may want to consider over time would be

- Creating Platform as a Service (PaaS) server options for frequently-used software stacks
- Adding additional server sizes. Currently we can create virtual servers up to the size of the physical servers they ride on. In the current solution, physical servers have 2x12-core processors and 256GB RAM.

Infrastructure Services (Sched. 4.3, Section 6.8)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPE is rated as a Leader in the Gartner Magic Quadrant for Infrastructure Utility Services in North America from 2011 through 2015.

As described in the previous section, HPES will continue to provide infrastructure services such hardware, software, network resources and services required for the existence, operation and management of the County IT and telecommunications enterprise, at both Plano and Tulsa until the data center consolidation is complete. These infrastructure services provide the foundation that supports County end users, third parties, and constituents. The infrastructure services environment is comprised of the hardware, software, storage and support services that underpin the operations of the applications and Dev/Test environments, including:

- Server environments that run the supporting tools, listed in the other sections of this proposal, including Service Portal, ITSM systems, monitoring, reporting, analysis and alerting systems.

- Infrastructure that provides software distribution and delivery services for mobile, desktop, and data center server environments.
- Local file and print services, distributed throughout County locations.
- Network infrastructure supporting the data center, such as load balancers, WAN Accelerators and global traffic managers (GTMs).
- Background services for applications, such as backups, batch processing and File Transport Protocol (FTP) services.

These services are described throughout the proposal; infrastructure services makes sure that these services are delivered in a consistent and unified fashion, providing a high quality of service to the County.

As with the application infrastructure, the servers for infrastructure services will reside in both the MPC and traditional hosted environment. This is based purely on the existing hardware and software platforms; however, over time, we will work to optimize and standardize this environment as opportunities arise. Servers that support infrastructure services receive the same supporting functions (such as performance and capacity management, and backup and restore) as application servers. Since these services underpin so many others, we make sure that no single points of failure exist that could potentially impact the availability of applications or facilities that support County business.

We perform comprehensive infrastructure testing for all components in an integrated environment for compute, storage, network, and database in a physical or virtual environment. We will maintain documentation that identifies all infrastructure services' hardware versions and software version life cycles so that we may adequately plan timeframes and completion dates to stay within supported versions of both hardware and software. We will also track hardware and software assets to adhere to the County refresh cycle. Note that the ESX servers and network components that comprise the MPC will be refreshed on the same schedule (20% per year) as their traditional hosting/network counterparts.

HPES will deliver skilled operations and engineering expertise to manage and monitor the infrastructure services environment, and apply automation to all processes to the greatest extent possible. For example, we deploy monitoring, antivirus, and policy compliance agents as part of the automated workflows. We manage the County's server, storage, backup, and networking resource pools and system management software, to facilitate daily operational support.

HPES will manage and maintain the County's server (compute), storage, backup, network, and security environments. We follow ITIL-aligned processes to determine critical business impact to component or system failures in infrastructure services, and to continuously analyze, identify and remediate single points of failure in infrastructure services.

Computing Services—We will install, fully manage, and monitor the operating system (OS) instance and the underlying virtual or physical server. We also maintain the health of infrastructure assets included in the solution, including server, storage, backup, network, and other devices.

In the MPC and traditional hosted environments, we will preconfigure the OS image for automated provisioning, provide OS patching and ongoing maintenance including performing all software installations, patching, and ongoing maintenance, and monitor system availability and security. We will perform root-cause analysis and corrective action of OS, physical and virtual servers, storage, backup and network environment problems, and all other IT Service Management functions.

End-User Software Distribution – HPES will design, deploy, and maintain software distribution infrastructure and services for end-user computing services and integrate and perform software delivery for County desktop and mobile devices. Our infrastructure services include support for devices on the County Public Library private network.

Operating System Software Support—We will provide a standard build for, then monitor and manage, virtual and physical operating systems such as Microsoft Windows, Red Hat Enterprise Linux and Oracle Solaris. We also support other types of UNIX operating systems and VMware as well as other hypervisors.

Storage services—We will use the HPE 3PAR enterprise storage, which is designed for both cloud and traditional environments. The storage hosts operating system images, virtual snapshots, and application data. All operating system images for virtual machines boot/reboot from the Storage Area Network (SAN). This architecture enables the server image to be disassociated from the physical hardware, allowing the image move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover for improved availability. Details on the storage architecture for the County are included in our response to Storage services (Sched. 4.3, Section 6.12).

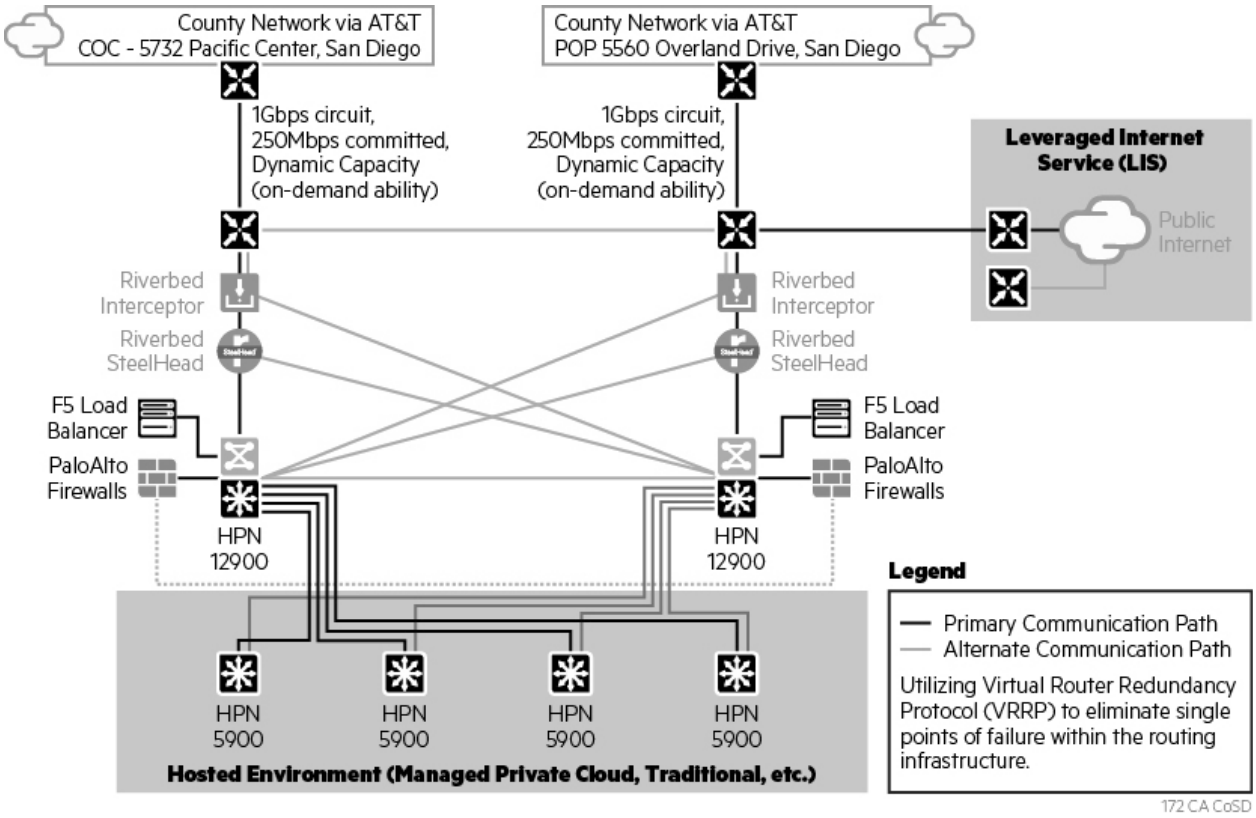
Backup and Restore Services—Backup services for virtual and physical computing services, provide operating system and filesystem (offline) backup for computing services to enable data restoration after a data loss event. Backups are accomplished by copying the specific data to backup media. We will perform the following:

- Provision backup infrastructure and backup software
- Perform backup management
- Maintain the backup schedule
- Review backup job completion status
- Intervene in the event of backup error
- Store data on disk
- Performs OS, file system, and database restore.

Details of County-specific backup and recovery services are described in response to Schedule 4.3, Section 6.13.

HPES will initiate and perform on-demand backups of the County environment. Shortly after the request is submitted, an incremental backup begins. For virtual servers, HPES can conduct regular snapshot backups of each virtual server instance, with the most recent snapshot being retained for recovery purposes. The snapshot feature backs up the OS disk and all attached data disks Figure 108 illustrates the data center network architecture.

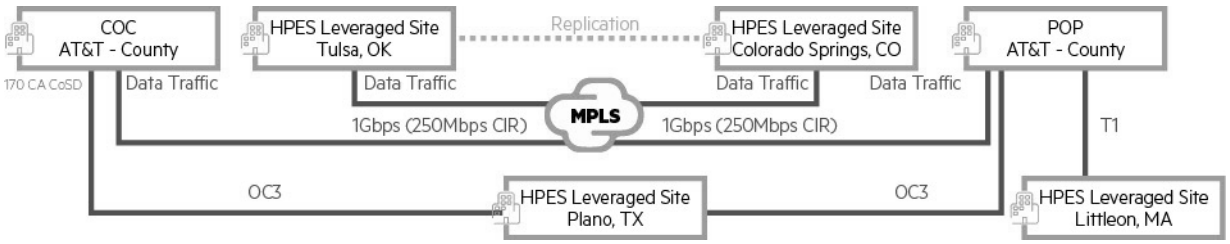
Figure 108. Data Center Network Detail



Our logical network architecture provides redundant network devices and data paths at every layer within the network infrastructure to protect against prolonged loss and enables HPES to maintain consistent and continuous service.

The physical network is the foundation for a successful data center operation. HPES provides a wide area network service construct enabling delivery of multiple telecommunications providers with diverse paths and entry points into each data center at our Tulsa, Oklahoma, and Colorado Springs, Colorado, locations. All circuits will be in an Active configuration to allow operation. Multiprotocol Label Switching (MPLS) circuits with a 250Mbps committed information rate (CIR) are used to connect our data centers to the County's Pacific Center and Overland Drive locations. Each of these circuits allows bursting above the CIR to provide on-demand bandwidth increases. Replication occurs between the two HPES data centers via a dedicated 10GB circuit. Figure 109 illustrates this connectivity.

Figure 109. Data Center Connectivity to the County Network.



The MPLS connectivity between the County and the Data Centers is fully redundant and scalable.

Our WAN and LAN network infrastructure will deliver multiple, active network paths with 1+1 redundancy at a minimum, whereby multiple components can fail without impacting end-to-end network availability. This enables us to deliver an environment truly capable of targeting 100% availability.

Scalability is delivered through the 1+1 active/active construct. We will use the HPE 12900 and 5900 series switches to provide a high performance, scalable, and open architecture designed for the County to leverage for the next decade. The platform is purpose-built for the data center around the principles of modularity, extensibility, and agility.

The network is designed with, and will be implemented with, modularity. This enables us to expand in the future in accordance with the forecast workload. It also simplifies network deployment activities. Our proposed solution will provide an environment with inherent High Availability capabilities, which is concurrently maintainable, and simple and efficient to operate, reducing the risk of administrative error.

In addition to our LAN and WAN infrastructure, we provide a Leveraged Internet Service (LIS). LIS simplifies Internet access into the data center hosting environments at a fraction of the cost of dedicated MPLS circuits. This resilient, shared Internet access offers a selection of data rates to match your speed and performance requirements and can be rapidly activated.

Connectivity from the County network to the Plano and Littleton data centers, required to remain post-transition to support the mainframe environment, is depicted in the diagram above; this connectivity will remain in place for as long as required to support the mainframe, and will be decommissioned once the mainframe applications are replaced

HPES' LIS is very different from standard commercial ISP access. It uses circuits from redundant ISP providers, terminated on hardened data center infrastructure to maximize reliability.

LIS is offered in monthly subscriptions from 1Mbps to 10Gbps for access to applications and servers hosted within HPES Data Centers. For implementation during Transition, we will deploy 50 Mbps, consistent with current traffic requirements in Plano and Tulsa; this will automatically surge if needed, with no additional charges to the County for surge usage.

Network Management Services—Comprehensive network design and infrastructure management services enable provisioning of up to 1024 VLANs per server; monitoring and management of data; and converged networks. Using our globally consistent, integrated network management standards, processes, and tools, HPES will implement new network technologies across the enterprise, manage disparate networks, and maintain reliable network performance. Our network management services provide a centralized and standardized system that automates network management of end-user data, security, and distributed resources. We will continuously monitor and maintain all load balancers for optimal operational performance. We will also deploy and maintain application and network acceleration in the delivery of the Services.

Security Services—Antivirus agents are automatically deployed and activated in an automated workflow when a server is deployed. Security policy compliance checks system configurations against security standards at a predefined scan frequency based on HPES security best practices. We will automatically load policy compliance agents as part of the deployment workflow and maintain and manage the security software, antivirus and policy compliance agents, antivirus definitions, and underlying infrastructure to support the security technology. HPES will maintain and provide all infrastructure security components including IPS and firewalls. Additional information is provided in response to Security Services (Schedule 4.3, Section 6.5).

Data Center Facilities Services—We will design all the key supply components (for example, power, air conditioning, and wiring) to be redundant. In addition, we will control access to the data center to prevent

unauthorized entry, and provide a robust infrastructure that provides adequate resistance to damage by the elements.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES has substantial experience in providing infrastructure services, as it does today for County applications in our Tulsa and Plano data centers, which will be consolidated into a single production data center in Tulsa, approximately nine months after contract award. Our data center staff in Tulsa, the HPES local support team in San Diego, and our virtual team of SMEs, located throughout the continental U.S., will provide ongoing operations and maintenance of the County's infrastructure.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES builds robust quality into infrastructure service delivery to achieve a high level of customer satisfaction. We operate the Tulsa datacenter in accordance with ISO 27001 and the ITIL framework and best practices. To manage County infrastructure environments, HPES follows ITIL-based service management (event management, and others) best practices.

HPES is a leader in ITIL service management principles, with 17,000 HPES ITIL-certified employees. Our ongoing process audits and metrics program provides visibility into trends, resulting in Continuous Service/Process Improvement (CSI/CPI) initiatives.

HPES and ITIL

- HPES co-authored the initial ITIL industry standards and continues to invest in the standards body today.
- We use standard ITIL-based processes and automated workflows, which we implement in many ITSM suites to deliver high-quality, cost-effective infrastructure services on a global scale.
- Our methods and techniques align with ITIL, ISO 20000:2011, and CMMI-DEV principles, as well as industry best practices.
- HPES has 17,000+ personnel certified in ITIL and supporting Government clients.

As noted above in the applications infrastructure section, (Sched. 4.3, Section 6.7) we will put in place a process and roadmap to continue unifying and integrating the various providers of services, and develop decision criteria that target workloads with specific characteristics for a specific type of service provider. HPES already has general guidelines and recommendations in place for this, which will be customized to meet County requirements. In addition, continual improvement will include convergence of tools for a more integrated data center services catalog and more self-service. HPES will provide additional self-service capabilities from the Service Portal at the County's pace. In addition, more standardization will help us improve the speed of delivery. With standardization comes the opportunity to automate things that are the same and occur repeatedly, which leads to more efficient provisioning and management than when each server must be uniquely configured.

For all infrastructure environments, whether provided in the MPC, traditional hosted, or other cloud environments, HPES provides a robust support service, to include the following processes.

- Hardware installation and configuration
- Hardware and firmware management and support
- OS and layered software product installation and subsequent patching and release management
- Supplier maintenance agreements and coordination of suppliers' activities in support of the applications infrastructure
- Capacity and performance monitoring and management
- Problem monitoring, including proactive hardware support
- Data center facility (floor space, power supply, cooling, wiring) services

- Network integration into the Tulsa data center
- Underpinning services that use the infrastructure services framework (such as directory and domain name management services), described in Section 2.5.
- Refresh of hardware components, at 25% per year for Windows environments and 20% per year for UNIX, Linux, and VMware ESX environments (MPC hardware is included).

Note that these services are provided for applications infrastructure, infrastructure services, and development and test services. The work instruction documents for these processes are available to the County in their current form. For the new contract, they will be updated to meet the specifics of the new solution and posted to the Service Portal for accessibility by County authorized personnel.

- Automated Tools – Automated systems and tools involved in proposed solution

The same tools described in the application Infrastructure Services section are used to manage the servers in the infrastructure services environment.

Tools used for support of software distribution for the end-user services framework are described in Section 2.7, in response to Schedule 4.3, Section 4.6.

Tools for backup, storage, network, security and other infrastructure components are discussed in the sections that address those framework components.

- Qualifications and Experience – Background and experience in comparable environments

HPES currently performs all required infrastructure services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: HPES manages and hosts DHCP services for all the County facilities within the data center. We manage:

- External and internal AD-based DNS services
- The County's Websense proxy and content filtering solution.

We use SCCM for software pushes to County desktops and laptops and HPE Server Automation to manage more than 1,300 County servers, both inside and outside of the data center. We apply the County's requirements and customizations on a gold disk image for use on servers and desktops. We manage the County's AD federated services and Oracle identity management for County applications.

SCCM is used to automate refreshes and updates and manage the overall deployed configuration. In addition, it controls and identifies users installing unauthorized software or authorized software in unauthorized configurations.

The County has more than 15,000 HPES-managed devices (desktops and laptops), for which we provides a standard operating system, core software, and catalog and portfolio applications. During the past 10 years, Microsoft tools have been used to create the image to distribute software and patches to these devices. Those tools included Active Directory, SMS, and SCCM 2007 for software distribution and device management along with MDT/OSD for OS imaging. Software refresh includes updates to the OS and applications.

Under the current contract we are upgrading to SCCM 2016 to provide additional functionality, such as newer operating systems for managed devices, and take advantage of enhancements in the product including improvements to the GUI, monitoring device health, remediating client issues, and deployment of SCCM to the Library domain.

U.S. Navy Marine Corps Intranet (NMCI): HPES established a centrally managed, secure application hosting environment to support enterprise applications. Our managed hosting support includes solution development, migration/engineering assessment, service preparation and setup, facilities and inventory, server management, client services, database management, application administration, storage management, applications hosting network hosting services, information security services, and DR. We manage 4,400 enterprise-wide servers and 1,183 virtualized servers running at 27 different virtualized sites. We operate and maintain the Next Generation Enterprise Network (NGEN) classified and unclassified storage capabilities including software, hardware, processes, and tools to facilitate the management and reporting of different classes of storage services across a wide range of workloads and applications.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Development and Test Services (Sched. 4.3, Section 6.9)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Our solution for the County's Dev/Test services[1] will take advantage of the hybrid infrastructure approach described in the previous two sections, employing both the MPC and traditional hosted environments, with resource pools separate from application infrastructure and infrastructure services. This approach provides the unified consistent architecture that makes sure the Dev/Test will provide an accurate picture of how an application's production environment performs. It also minimizes disruption to the current environment and leverages the County's current investment in traditional infrastructure; yet still achieve the benefits of on-demand private cloud services. The MPC environment is a highly standardized environment with high redundancy and high availability to eliminate single points of failure. Moving to MPC will provide streamlined server provisioning, enabling HPES to provision, scale, and de-provision virtual servers in hours instead of days, once approved by the County. It will also include tools that simplify capacity and performance management, monitoring, patching, and security and regulatory compliance.

This hybrid approach leverages the existing traditional infrastructure environment in Tulsa, including people, processes and tools. Both the MPC and the traditional hosted infrastructure are sized to accommodate the combined workloads from Plano and Tulsa.

The MPC environment designed for the County will provide the following benefits for Dev/Test:

- For Applications maintenance and operations (M&O), dynamic and persistent resources provide a cost-effective solution for certain P1/P2 category applications, we propose keeping persistent environments in place, to support rapid test cases, such as performing testing of production fixes in response to

[1] We use the term "Dev/Test" to refer to any and all nonproduction environments, recognizing that there are multiple types of test environments that the County uses , such as user acceptance testing, system integration testing, and so on. Also note that the Dev/Test environment described here will include environments for new development projects as well as for supporting Applications M&O (aka Break/Fix).

incidents. A list of P1/P2 applications that will initially have persistent Dev/Test environments in the MPC is provided in Table 55. This list is valid as of the time of the original proposal analysis. During Transition, the list will be updated and finalized, based on the state of the applications at that time. P1/P2 applications that have been stable for a long time and are not often updated may only need dynamic environments. For these, as well as all P3/P4/P5 environments, we propose taking advantage of MPC's elasticity, where we dynamically scale the County's secure, dedicated virtual infrastructure up and down as needed quickly and easily by obtaining and releasing IT computing resources on demand.

- Faster provisioning of hosted application services, and cold storage of dynamic virtual images not in use helps the County to avoid operational costs and data center footprint associated with paying per-server for idle servers.
- Enhanced scalability and flexibility to adapt to the County's dynamic business demands.
- Security, privacy, and compliance—the MPC infrastructure is 100% dedicated to the County and HPES protects this behind a highly secure data center firewall. We deploy and manage the technology based on our extensive security testing practices that meet multi-segment security standards and compliance beginning with FedRAMP Moderate requirements.
- Access to the latest cloud innovations when the County is ready. HPES helps the County stay at the forefront of this technology by continuing to offer service and technology enhancements as HPE Labs research and develop next generation cloud systems.
- Integrated with County identity and access management services either through Active Directory or Oracle IDAM.

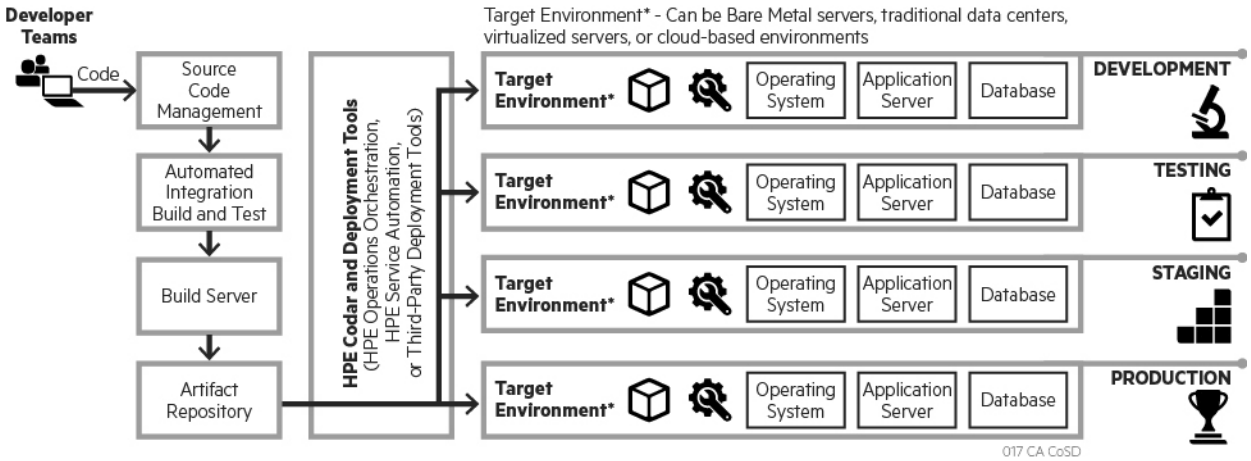
The Dev/Test environment is designed to meet County goals for continual improvement and cost effective innovative services to help the County transition to a marketplace of hybrid-provided services governed by Reports 49/50 standards and County IT strategy. Financial governance of the Dev/Test environment will be through the HMCB and will provide visibility across the hybrid environment to all Dev/Test resources in MPC and traditional hosted environments as well as public cloud environments, if required in the future.

Underlying technical parameters and processes needed for VM deployment, configuration, capacity management, patching and VM life cycle management comes from our experience building the current Rancho Bernardo Dev/Test lab. Our solution will build on those experiences using the VMware automation built into the HPE Helion Cloud tools, and will increase the County's readiness to adopt further automation such as HPE Codar and DevOps methods as described further in this section.

To further increase the level of automation and improve the Dev/Test environment builds, our strategy is to mature the cloud development, orchestration and delivery tools that will enable Dev/Test environments to be quickly placed through one-click deployments, automatic rollbacks, and applications promoted across virtual environments. Our goal is to establish modeled environments that will enable additional consistency through our automated tools such as HPE Codar and HPE Cloud Automation solution for version-controlled, one-click deployments, rollbacks and promotions. Figure 110 below illustrates sample scenarios in which automated tools can execute deployment of environment models into traditional data centers or third-party private, public, or hybrid clouds.

Employing the same architecture used in application infrastructure services for Dev/Test will streamline and simplify the migration of applications—from Dev/Test to production. We will ensure that all individual technical components configured with or added to the services mesh together to achieve the intended results prior to release to the production environment. We will operate the Dev/Test environment according to all County standards and in close alignment with the production environment. When permitted by the County, we will use the VMware integration capability of the MPC and HMCB to clone production images to the test/dev environment. This enables us to build accurate Dev/Test images that reflect current production data quickly and efficiently.

Figure 110. Automated Tools for Deployment of Environment Models



HPE's 3PAR unit, American Airlines, and Vodafone currently use our continuous integration tools to automate the version-controlled modeling and one-click deployments, rollbacks, and build promotions across development, test, and production environments.

Our v 4.0 MPC solution is a commercial-release offering and is designed as a set of building blocks that can be sized and deployed to fit almost any enterprise's requirements. The building block architecture and the integration with industry-leading virtualization tools such as VMware, make the design inherently reusable. After we implement the MPC infrastructure, we will then be able to reuse the same infrastructure technology and processes to scale up or scale out existing workloads, and add new workloads. Additionally, when the capacity of the MPC environment is reached, we can scale out the environment by adding building blocks of servers, storage, and network without replacing the current investment.

We will have sufficient SAN capacity in the Dev/Test environment for MPC to store cold virtual machine image files. We will manage Dev/Test workloads within a SAN-based repository visible to the private cloud and perform tasks such as boot up and shut down of virtual machine images on-demand. Upon the County's request/approval, the tasks will commence automatically. The Dev/Test environment will have interfaces enabling connectivity to the production environment as needed to meet business needs. We will secure these interfaces with VLANs and access control lists. Identity access management services will be applied across all County environments, including Dev/Test. These services are described further in our response to Schedule 4.3, Section 2.18 contained in Section 2.5 of this proposal.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The Dev/Test environment is part of the overall hybrid data center architecture and will reside in the Tulsa data center.

The Rancho Bernardo lab remains available for integration and testing services and proof-of-concept applications or infrastructure that need to be isolated from the production network.

Resources working in the Dev/Test environment include HPES project managers (PMs), developers, and operations staff, as well as designated County stakeholders during user testing phases.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

The methodologies and processes used to manage the Dev/Test Service are the same as those described previously in the Infrastructure Services in response to Schedule 4.3 Section 6.8.

As described in the Solution Summary section above, HPES uses the following methodologies:

- IT Strategy and Architecture (ITSA)
- ITIL framework

ITSA

- HPES methodology for developing solutions and architectures
- Structured, participatory approach that involves key stakeholders
- Proven effective through years of experience in defining, guiding, and managing complex environments in multiple application domains

As a continual improvement initiative, HPES and the County will consider adopting development and operations (DevOps) approach to managing development. HPES will incorporate DevOps practices of collaboration, source control, deployments through version-controlled models, and system configurations. DevOps work together to design and maintain models and configurations in version control from which automated tools can fetch and deploy. These practices facilitate consistency across environments, maintain audit trails of changes, and provide early feedback to developers resulting in higher quality and reduced risk. DevOps, and the pros and cons for its use, are discussed in greater detail in Section 2.10.

New processes and process changes for provisioning and managing server infrastructure in the hybrid environment are the same for all types of servers, and are described in the Infrastructure Services section above. In addition, specific to the Dev/Test environment, the HPES team will create new processes for:

- **Automated Release Management** – Using the approach described in the Solution Summary section above and illustrated in **Error! Reference source not found.**.
- **Dynamic Image Management –** Used for turning up and down dynamic images and making sure that cold-stored images are reused when appropriate (as opposed to creating new images every time) and processes for inventorying and removing cold-stored images. For physical servers, images are not dynamic, but if an environment is targeted for turn-down so that its resources may be reused for another project, we will have processes and scripts to back it up and remove it from active support status during the time while no projects are using its resources.

When a Dev/Test team needs an environment to support a new release, for example, they will submit a request for requisite resources through the cloud interface or the traditional request process, depending on the resource needed. Upon approval of the request, and determination that sufficient capacity is available to support it, the resources will be automatically provisioned in the cloud or the traditional VMware environment (or provisioned with task-level automation in the traditional hosting environment) and the requesting team notified of its availability, measured in hours, not months.

The primary benefit of our approach—allowing our DevOps teams to focus on continual service delivery, providing the County confidence we can deliver on business outcomes—results from HPES' in-depth and extensive knowledge of the County's applications and IT environments.

- Automated Tools – Automated systems and tools involved in proposed solution

The primary tools used to provision and manage the Dev/Test environment are described in the Application Infrastructure Services Section above. For version-controlled, one-click deployments, rollbacks and promotions, we will also use HPE Codar.

- Qualifications and Experience – Background and experience in comparable environments

HPES currently provides Dev/Test services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: Under the current contract with the County, HPES provides the following types of Dev/Test environments:

- **Traditional Data Center:** Under this model, HPES provisions virtual servers on the County environment in the Plano/Tulsa data centers using base-lined and security-hardened gold images suitable for the County. This model prioritizes ITIL processes based on security, service level, availability, and support through standardized procedures in deployment, configuration, monitoring, patching, and virtual machine (VM) life cycle management.
- **Platform as a Service (PaaS):** In 2013, we built a prototype of a private Dev/Test cloud in the Rancho Bernardo environment to provide County application teams the ability to rapidly build, develop, and run proof-of-concept trials without the complexity of provisioning and maintaining infrastructure associated with the traditional data center model. The Rancho Bernardo PaaS environment provides preconfigured, on-demand instances of application servers, web servers, databases, and middle-tier components in a container-based model. The emphasis is to accelerate "idea to value."
- **Platform as a Service (PaaS) on HPES Helion Platform:** In 2014, the County began Helion Virtual Private Cloud (VPC), a purpose-built Government community cloud, when the Land Use and Environment Group (LUEG) enabled its Beach & Water web application. With the assumption that more County applications could move to VPC, HPES replicated the County's production, test, and development VLAN structure to provide network symmetry. Our plan is to continue to migrate and expand capabilities over time by establishing a virtual private network (VPN) tunnel to complement delivery options and integration between Tulsa/Plano, Rancho Bernardo, and the Helion Cloud.

California Department of Corrections and Rehabilitation (CDCR): HPES partnered with Marquis Software Development, Inc. to deliver the Marquis electronic Offender Management Information System (eOMIS), an enterprise-wide offender management solution providing a comprehensive, module based solution for inmate management and community supervision.

These solution includes the following activities and tasks:

- Architecting, installing, and operating system hardware and software to support the application development life cycle (such as development, testing, training, performance testing, production support, and production)
- Conduct system testing, performance testing, and integration testing of the solution
- Provide requirements elaboration and traceability
- Conduct design sessions to define customizations of the COTS offender management system necessary to meet specific needs of CDCR
- Develop web-based training and lead customer facing training sessions
- Conduct on-site readiness assessments at 33 State prisons in preparation for deploying the solution
- Provide 24x7 production support.

Defense Health Agency: HPES manages the worldwide SVHE server hosting platform for the Military Health System (MHS) with more than 3,075 active provisioned servers. In addition, the team manages a development environment at the Development & Test Center (DTC) with 137+ servers provisioned.

HUD: We planned, engineered, coordinated, and executed a flawless transition of HUD's production applications and their development and test environments seamlessly and without interruption. We completed a complex, 6-month transition project on time, under budget.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

An alternative approach, to increase standardization and advance the County's "virtual first" objective, is described in the Price Volume. This is not an alternative technical solution, but an alternative way to package Dev/Test services.

E-mail Services (Sched. 4.3, Section 6.10)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Recognizing the criticality of email as a productivity tool for County employees in conducting business, migration to Office 365 (O365) Exchange Online will give County employees access to the latest features and functions available. As email services have grown in importance over the years, we fully understand the necessity of maintaining uptime and keeping the platform operating consistently so that County employees can do their jobs effectively and in a timely manner. HPES will migrate the existing, traditional-hosted Exchange 2010 email to O365 Exchange Online as a transition project, as detailed in Section 2.11.

HPES will continue to manage the current Exchange 2010 high availability environment for email service that includes four Exchange servers each in Plano and Tulsa. Our support will include mailbox management, OWA traffic, ActiveSync, mail relays, and RightFax. We will provide backup and restore functions as we do today, and meet special mailbox recovery and journaling requirements. We will also continue to meet the current retention requirements of 118 days for deleted items and mailboxes and perform backups every other week and retain tapes for 2 weeks before overwriting.

HPES will begin planning for the email migration to O365 Exchange online, housed in the Microsoft Government Community Cloud, as described in the Resource and Facility Approach Summary section below. O365 fully meets the County's requirements for email services and allows the County to take advantage of additional available functionality in a timeframe convenient.

We are using the County's current volume of 13,000 O365 subscriptions. A full discussion of NetBond is provided in Section 2.8, Network Services Framework.

Rationale: O365 Exchange Online reduces the need for hosted server-based solutions and enables the efficiency and flexibility of a cloud-based offering. The Microsoft Government Community Cloud is a US-based, ITAR-compliant solution for Government entities.

The transition to Exchange Online will result in the following changes to the existing environment:

- One hybrid exchange server in Tulsa to maintain the local distribution lists
- The Rightfax servers in Tulsa will be connected to redundant local SMTP relays
- Microsoft will provide email archiving, journaling and e-discovery services.

Recognizing that break/fix is a top priority, support for email will continue exactly as it is now, even after the transition to O365. The HPES Service Desk will own the trouble tickets and resolution from start to finish. We are unique in the industry because of our tight integration with Microsoft, which helps us to deliver responsive support throughout the trouble reporting process. HPES support personnel are collocated in Redmond, WA with Microsoft engineers, allowing close contact on a daily basis. HPES and

Microsoft will use our ticketing system that is devoted to HPES client support to meet the County's required SLs.

The following table illustrates how Microsoft Exchange Online meets the requirements of the RFP.

Table 56a. Microsoft Exchange Online and Office 365 Features

Requirement	Solution
With respect to licensing, the County has a Microsoft Enterprise Agreement (EA) in place that includes Office 365. The Microsoft EA also includes licensing for the data center Exchange servers.	Our solution covers the County's existing subscription with Microsoft.
Migrate to the current version of Exchange	All MS office productivity applications such as Outlook are continually updated and patched to the most current version. During the migration to Exchange Online, End -Users will be updated to the latest version of Office 365 Professional Plus. Office 365 Professional Plus will be installed on all End-User devices as a part of Transition
Migrate to the current version of Outlook to desktops	
Contractor shall ensure high delivery of cloud based E-Mail Services and complete End-User integration.	
Maintain versions of Exchange within 12 months of new releases	
Maintain patch levels of Exchange within 3 months of any new release	
Maintain County retention policies (60 days) without exception	Retention limits can be set across the board or down to an individual mailbox. A County-requested legal hold would be the only exception to the retention policy.
Unlimited Mailbox storage	HPES will configure the mailbox to use the archive as the mailbox location to provide unlimited storage.
Unlimited user archive storage	
Redundancy built-in to insure minimal down time for E-Mail user	MS Office 365 (including Exchange Online) provides 99.95% availability. Their infrastructure is architected with sufficient redundancy and replication to support this level of availability with no data loss due to failures; HPES and AT&T provide redundancy of network and surrounding components.
Continuous backup to prevent failure due to data loss	
Contractor shall maintain E-Mail Services so there is not a single point failure thereby assuring County daily use continues to operate during any unplanned event or outage.	
Malware and anti-spam protection at the perimeter and within the Outlook client	Exchange Online Protection (EOP) is included in our solution and provides malware and anti-spam protection at the perimeter and within the server. Malware protection at the desktop is provided by Symantec Endpoint Protection. EOP also provides the following capabilities: - Journaling - E-Discovery - Archiving - Data Loss Prevention Additional information about Exchange Online security is provided below this table.
Immutably preserve or In-Place Hold for user data, as requested	
Protection against unsafe attachments at the perimeter and the Outlook client	
Data Loss Prevention implemented per County policy	
E-discovery implemented and used as requested by the County	
Migration of PST files to Exchange archive	

Requirement	Solution
Elimination of PST files from End-User environment	The capability to import PSTs in support of eliminating them from the local environment is available. We will provide migration of End-Users' PSTs
Implement Outlook Web Access (OWA)	portal.office.com is the Office 365 replacement for OWA—this is provided as part of the implementation during transition. Portal.office.com will only be accessible using County credentials. The process to enforce policy parameters on OWA is described below.
Lockdown OWA to further protect County information	
Mobile aware and productivity included	Microsoft offers a mobile application suite, including Outlook, or users can access portal.office.com via mobile. The same security capabilities apply.
Contractor shall establish and maintain global directory and synchronize E-Mail directories with all County Departments (e.g. Sheriff, District Attorney, SDCERA) or as specified by the County.	Synchronization is accomplished via Azure AD Connect, which we have already implemented for County users. Additional user groups will be added to the synchronization prior to migrating their mailboxes.
Complete migration of all active E-Mail users	Our transition plan will migrate all active email users
Contractor shall integrate fax capabilities into E-Mail Services for End-Users	We will integrate the current RightFax solution with Office 365 using a hybrid Exchange server and SMTP relay in the Tulsa Data Center.
Contractor shall recommend a plan for County approval, and execute the approved plan for integrated digital signing to all mailboxes leveraging County PKI platform.	S/MIME is supported and configurable in Office 365.
Contractor shall recommend a plan for County approval, and execute the approved plan for integrated encryption services on all mailboxes based on leveraging the County PKI platform.	Encryption is provided in Office 365 and can be integrated with CoSign and/or the Symantec solution; we will provide a plan post-migration for County approval.
Contractor shall ensure through continuous review and report that all End-User mailboxes comply with the County's E-Mail retention policy.	Exchange Online provides administrative reporting and auditing that meets this requirement
Contractor shall recommend a plan for County approval, and execute the approved plan to send encrypted E-Mails to E-Mail addresses outside of the County network.	Cloud File Management provides integration into Outlook, which allows transmission of encrypted content to internal or external recipients which require authentication. Exchange Online Data Loss Prevention (DLP) also provides expiration of protected email and content. Cloud File Management has an "I forgot my password" function to enable self-service reset.
Contractor shall recommend a plan for County approval, and execute the approved plan for the ability of external recipients of encrypted E-Mails with access to encrypted content via an authentication.	
Contractor shall enable End-Users an expiration date for sent encrypted E-Mail messages.	
Contractor shall provide self-help password administration for recipients of encrypted E-Mails that permit passwords to be established and reset.	

Requirement	Solution
Contractor shall maintain a timeline/roadmap of all E-Mail Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.	For the Office 365 Pro Plus environment, Microsoft typically releases updates on the second Tuesday of each month to the Internet. Microsoft publishes an Office 365 public roadmap that provides visibility into upcoming releases to the cloud environment. We will maintain a timeline/roadmap of all email integrated hardware and software that support this schedule and release the Office 365 Pro Plus updates to the County end-user environment according to that schedule. A detailed description of the update process is available on Microsoft TechNet: https://technet.microsoft.com/en-us/library/dn761709.aspx and the public roadmap is available here: http://fasttrack.microsoft.com/roadmap Exchange Online updates are released quarterly. More information about Microsoft's update process for Exchange Online is available at https://technet.microsoft.com/en-us/library/jj907309(v=exchg.160).aspx
Contractor shall provide centralized support and tools for E-Mail Services hosted within the data center or hosted outside the data center.	Our Service Desk will provide the single point of contact for all email support, including Office 365 and all surrounding infrastructure, such as network, firewalls, fax equipment, and other supporting components. Through our enhanced support service, we provide agents co-located with Microsoft support teams to make sure that issues that need to be escalated with them are not simply dispatched but are followed through to completion.
Contractor shall maintain and be responsible for all components needed to provide E-Mail Services (e.g. load balancers, firewalls, IPS).	
Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to E-Mail Services.	Our Architecture and Engineering team will provide these services, in coordination with our Portfolio teams, Microsoft, and our other suppliers/partners such as AT&T, Symantec, and RightFax.
Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security	

Office 365 Exchange Online Security

Encryption in Exchange Online. Office 365 encrypts data while at rest on their servers and while in transit between End-Users and Office 365.

Data In Transit. Exchange Online supports certificates using Transport Security Layer (TLS) version 1.0 through 1.2, and has recently moved to Secure Hash Algorithm (SHA)-1 certificate support to SHA-2 (Microsoft began deprecating SHA-1 certificate support in June of this year). TLS 1.2 uses Advanced Encryption Standard (AES) with 256-bit length cipher key. Microsoft begins with the strongest cipher key and algorithm and negotiates the proper level with the receiver. There are three types of encryption options with Exchange Online, as follows:

- Office Message Encryption (OME)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Information Rights Management (IRM).

Data At Rest. Email data at rest is encrypted using BitLocker Drive Encryption at Microsoft Government Community Cloud Data Centers on hardware using Trusted Platform Module (TPM) version 1.2.

Anti Malware and Anti Spam. Users on Exchange Online with Exchange Online protection have their email messages automatically protected against spam and malware. The service has built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect you from spam. Exchange Administrators do not need to set up or maintain the filtering technologies, which are enabled by default; however, we will make company-specific filtering customizations in the Exchange Admin Center (EAC) or via remote Windows PowerShell, as required.

Spam is prevented as follows:

- **Connection filtering:** Checks the reputation of the sender before allowing a message to get through. We are able to create an allow list, or safe sender list, to make sure that you receive every message sent to you from a specific IP address or IP address range. We can also create a list of IP addresses from which to block messages. Since your license includes Advanced Threat Protection (ATP), connection filtering is used by *spoof intelligence* to create allow and block lists of senders who might be trying to spoof your domain.
- **Spam filtering:** Checks for message characteristics consistent with spam. We can change what actions to take on messages identified as spam, and choose whether to filter messages written in specific languages, or sent from specific countries or regions. We can also turn on advanced spam filtering options if you want to pursue a more aggressive approach to spam filtering. Additionally, we can configure end-user spam notifications to inform users when messages intended for them were sent to quarantine instead. From these notifications, end users can release false positives and allow us to report them to Microsoft for analysis.

Office 365 Exchange Online can also monitor outgoing messages to determine whether they are assuming the characteristics of spam, and allow us to act quickly. We can further enhance spam filtering by creating custom Transport rules based on County policies. For example, we can use Transport rules to set the spam confidence level (SCL) value for messages that match specific conditions.

Malware is prevented in the following ways:

- **Layered Defenses Against Malware:** Multiple anti-malware scan engines help protect against both known and unknown threats. These engines include powerful heuristic detection to provide protection even during the early stages of a malware outbreak. This multi-engine approach has been shown to provide significantly more protection than using just one anti-malware engine.
- **Real-time Threat Response:** During some outbreaks, the Microsoft anti-malware team may have enough information about a virus or other form of malware to write sophisticated policy rules that detect the threat even before a definition is available from any of the engines used by the service. These rules are published to the global network every 2 hours to provide the County with an extra layer of protection against attacks.
- **Fast Anti-Malware Definition Deployment:** The Microsoft anti-malware team maintains close relationships with partners who develop anti-malware engines. As a result, the service can receive and integrate malware definitions and patches before they are publicly released. Our connection with these partners often enables us to develop our own remedies as well. The service checks for updated definitions for all anti-malware engines every hour.

As part of the County's Advanced Threat Protection (ATP) subscription, there are further protections available. ATP helps prevent zero-day malware attacks in your email environment. We are able to set up separate policies for ATP to check either links or attachments or both. Each policy can be applied to a specific set of End-Users, at County direction.

ATP aids in both email delivery and Web browsing from links in emails as follows:

- **Email Delivery**: If the safe attachments policy that applies to a particular recipient has an action of "Block," the email will not be delivered until the attachments can be detonated by the safe attachments technology in EOP. Safe attachments will launch a unique hypervisor to open the attachment. This can result in a delivery delay of 5 to 30 minutes for each mail evaluated by safe attachments.
- **Web Browsing (Safe Links)**: If a link points to a website recognized as not malicious, *Safe Links* adds very little latency to loading the target page. If the link points to a website recognized as malicious, the user is routed to a warning page and has to go through it (if click-through is enabled) to continue on to the site.

Exchange Online is a highly secure email platform with built-in encryption, anti-malware, and anti-spam. Any system is of course only as secure as its weakest link, and typically that link is at the client level. Microsoft has continually enhanced and hardened its mail clients, and Outlook on Windows as well as the Outlook app on mobile platforms is a highly secure portal to your email; we at HPES recommend users use these hardened clients insofar as possible.

Outlook Web Access (OWA) has been Microsoft's web-based email solution for years; because it has been optimized for multiple browsers and versions of HTML, it is perceived as being less secure than other ways to get email. We do not disagree with this perception. If one needs to use OWA, however, there are few methods to make its use more secure. The most secure way to access web-enabled clients is of course multi-factor authentication (MFA), but we acknowledge that MFA is not a preferred approach at the County, so we are not recommending it. Our recommendation therefore stands that, to maintain a highly secure email environment across the entire chain, it is most prudent to use Microsoft's dedicated client apps. For users who require OWA access, various limitations can be configured using the owamailboxpolicy parameters. For example, OWA on Office 365 Exchange Online can be configured to not allow downloading of any attachment while using OWA. It is configurable in two ways:

- via the GUI (basic on/off)
- via Powershell commands for owamailboxpolicy (which provides more options).

DirectFileAccessOnPublicComputersEnabled	Specifies left-click and other options available for attachments when the user has signed in to Outlook Web App from a computer outside of a private or corporate network. If this parameter is set to $true,Open and other options are available. If it's set to $false, the Open option is disabled.
DirectFileAccessOnPrivateComputersEnabled	
ForceWacViewingFirstOnPublicComputers	Specifies whether a user who signed in to Outlook Web App from a computer outside of a private or corporate network can open an Office file directly without first viewing it as a webpage.
ForceWacViewingFirstOnPrivateComputers	
ForceWebReadyDocumentViewingFirstOn PublicComputers	
ForceWebReadyDocumentViewingFirstOn PrivateComputers	Specifies whether a user who has signed in to Outlook Web App can open a document directly without first viewing it as a webpage.

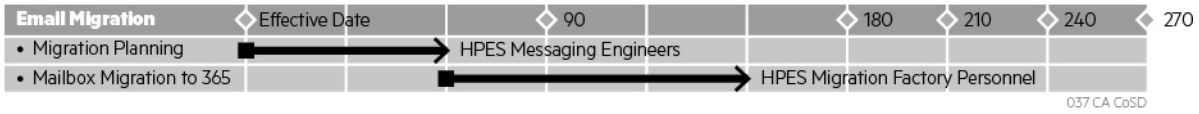
WacViewingOnPublicComputersEnabled	Specifies whether a user who has signed into Outlook Web App from a computer outside of the corporate network can view supported Office files using Outlook Web App.
WacViewingOnPrivateComputersEnabled	
WebReadyDocumentViewingOnPublic ComputersEnabled	
WebReadyDocumentViewingOnPrivate ComputersEnabled	Specifies whether WebReady Document Viewing is enabled when the user has signed in from a computer outside of the corporate network.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES' approach to O365 deployment is a repeatable process that we developed through numerous successful migrations, including the HPES corporate email transition. Referred to as the Migration Factory, it is a standardized service that uses specialized tools running on temporary servers to move email boxes from traditional Exchange servers to the Microsoft cloud. HPES will complete the migration virtually, and at the Tulsa data center.

The migration planning process, shown in Figure 111, which we anticipate to last 60 days, begins at the effective date of the contract with HPES messaging engineers assessing the environment, determining the migration infrastructure need, setting up the temporary infrastructure, and developing a mitigation strategy to address any identified issues. With the migration infrastructure in place, the Migration Factory takes over, moving over email boxes quickly and seamlessly. We expect the migration to occur during an 8–12 week period.

Figure 111. Email Migration Timeline



HPES' thorough upfront planning facilitates an accurate and timely email migration

HPES will provide project management support, as described in Section 2.5.7 (Sched 4.3, Section 2.9). Our PM will guide the process, and County personnel will be supported through the normal Service Desk for any issues that might arise from an end-user access standpoint.

HPES also provides Enhanced Support for Microsoft Office 365. This service is a bridge between our Standard Service Desk services and the services provided by Microsoft. This is a team that is located in Redmond, WA, with Microsoft. The table below provides a list of the services provided by that team, showing the delineation between HPES-provided support and support provided by Microsoft. The costs of these services are allocated between the Email RU and the User Data RU (Refer to Section 2.12, Transformation Services for a description of this Service).

Table 56b. HPES and Microsoft Support Responsibilities

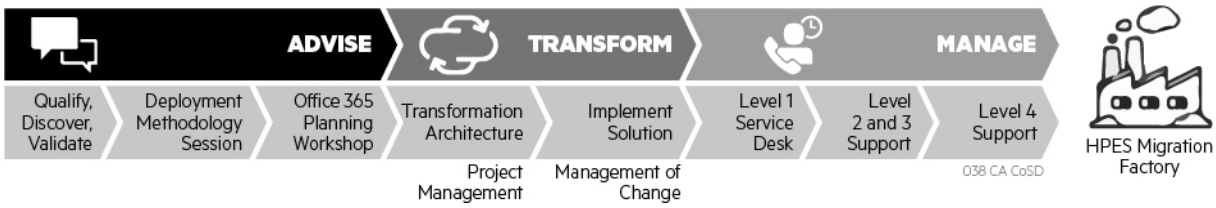
Roles or tasks	HPES	Microsoft
HPES and Microsoft Office 365 support team	– HPES presence in Microsoft Redmond office – Shared document repository – Knowledge databases, process documents, issue tracking – Weekly team meetings to review tickets, ongoing issues, planned changes, process improvements	
Office 365 service monitoring Microsoft initiated triage and incident ticket management	– Action tickets for hardware investigation and repair – Communicate any Office 365 service issues to the County	– Monitor services and platform, hardware, and network – Escalate ticket via case exchange to HPES
County or HPES initiated triage and incident ticket management	- Troubleshoot and provide resolution - Escalate via HPES and Microsoft case exchange - Communicate resolution to the County	– Responsible to troubleshoot and work with HPES to resolve the incident – Communicate the resolution to HPES
Post incident time line and summary	Communicate post incident and prior to release of Microsoft Post Incident Response (PIR)	Review time line and summary with HPES
Post incident response (PIR) and root-cause analysis	– Communicate to the County – Request Microsoft PIR on behalf of the County	– Responsible to develop PIR – Communicate with HPES
Reporting	– Active and inactive mailboxes – Types of mailbox connections – Mailbox usage and mail activity reports – Mailbox administration activity reports – Mail Security reports – Mailboxes marked for eDiscovery and Litigation Hold – OneDrive for Business sites deployed – OneDrive for Business storage	– Service level availability compliance – Incident reporting – Volume and resource utilization – Post Incident Response and root-cause analysis

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES' dedicated email migration practice is built on standardized processes, tools, and trained personnel to assess, prepare, implement and gracefully shut down Exchange migration projects.

The O365 Transformation methodology follows our standard advise, transform and manage, illustrated in Figure 112. . Messaging engineers conduct due diligence on the current environment, and prepare the infrastructure and tools that the Migration Factory personnel will use to move from Exchange 2010 to Exchange Online. As groups are migrated, we move into the manage phase, providing support for the entire Office 365 suite from our Service Desk to our HPES/Microsoft co-located support group in Redmond.

Figure 112. HPES Transformation Methodology



This proven process provides a structured approach to email migrations that minimizes disruption to email users.

HPES' Transition and Transformation Methodology has been honed as a result of our work with clients all over the world. Recently, HPES followed this process to accomplish our own internal email migration to cloud-based Office 365.

- Automated Tools – Automated systems and tools involved in proposed solution

Our Migration Factory uses a migration tool from Binary Tree Company to facilitate mailbox migrations.

- Qualifications and Experience – Background and experience in comparable environments

HPES currently provides all required email services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: We manage and operate the County's Microsoft Exchange farm and mail relays, which receive nearly 2.7 million emails weekly.

HPES Email Migration: HPES recently completed its corporate on premise Exchange migration to O365 Exchange Online for nearly 300,000 users worldwide. The resources who lead this migration now drive HPES' O365 client practice, bringing a proven level of expertise to support similar client migration activities.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Unified Communications Infrastructure Services (Sched. 4.3, Section 6.11)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The move to Office 365 Exchange Online opens the door to expanding cloud services to include unified communications, (UC) which provide greater flexibility than traditional data-center focused solutions. With this transition to O365, the vast majority of the County's email will come from Microsoft's Government Community Cloud, as well as the Lync/Skype for Business infrastructure.

Through our 30+ year partnership with Microsoft, we are deeply integrated in delivering UC infrastructure. Also, HPES and AT&T have jointly delivered UC to the County for more than a decade. This same team will implement the proposed UC solution to deliver these innovative services to the County.

While most end-user experience with UC is local the underlying functionality will be delivered from the Microsoft Government Community Cloud. AT&T will continue to support Avaya phones at the desk and from the AT&T POP in San Diego.

Hosting UC in the cloud the most-cost effective and technically feasible approach as this architecture is designed for Cloud Delivery.

Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Aside from a single hybrid Exchange server and an email relay in the Tulsa data center, almost all of the data center Services infrastructure for Unified Communications is in Microsoft's Government Community Cloud.

Microsoft's Government Community Cloud is an Office 365 service offered exclusively to U.S. Government entities. Some features of the Government Community Cloud are as follows:

- The County's content is stored within the U.S.
- Access to County content is restricted to screened Microsoft personnel.
- Office 365 Government complies with certifications and accreditations that are required for U.S. Public Sector (USPS) customers, such as FedRAMP Moderate.

Through the County's existing G3 O365 Subscription, the Government Community Cloud is already deployed. The current Lync functionality will be, by the end of transition, on O365 Exchange Online also.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Microsoft's internal cloud data center processes are ITIL-based. As part of Continual Service Improvement (CSI), Microsoft strives to achieve more efficient delivery, higher quality and innovative offerings.

- Automated Tools – Automated systems and tools involved in proposed solution

Inherent to the Microsoft Government Community cloud are the necessary tools to create and manage the services.

- Qualifications and Experience – Background and experience in comparable environments

HPES' qualifications include:

- Microsoft's Prime Integrator for Lync/Skype for Business
- HPE is Microsoft's largest OEM and Gold Certified Partner
- Named "Microsoft Global Enterprise Partner of the Year" five times.

HPES currently provides all required unified communications services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: We provide infrastructure support for Lync, WebEx, and Granicus web conferencing and Countywide broadcasts. We designed and support the County's Mutare Unified Messaging solution, enabling County executives to have voicemails transcribed into text. We also manage the desktop client of the County's Lync 2013 messaging environment, serving 13,000 users.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Storage Services (Sched. 4.3, Section 6.12)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

With the County's goal to obtain storage solutions that are flexible, affordable, and contribute to a reliable, predictable and efficient infrastructure, HPES' storage solution allows allocation of storage capacity as needed across various types of applications.

HPES designed the storage capacity to support Tier 1, Tier 2, and all dependent applications in the Tulsa data center using a dedicated SAN. The 3PAR P20000 has a small amount of Solid State Disk (SSD) storage for 3PAR metadata. Service storage tiers are provided as follows:

- Tier 1 storage in the Tulsa data center is configured using low cost 10,000 RPM drives, blended with 9.6 TB of flash storage, that are thickly provisioned and will provide higher performance at a lower cost than the current 3PAR with 15,000 RPM drives.
- Storage for Tier 2 applications, will use 10,000 RPM disk drives when thinly provisioned or combined with 7200 RPM disk drives.
- We will also use 7200 RPM disk drives for archive storage that includes low performance, end- user replicated or infrastructure services.

HPES will use the SAN 3PAR array to develop, install, and maintain Wintel and UNIX application infrastructure storage. In some cases, direct attached storage may be required for ongoing service support. We will work with the County to develop plans to migrate all services requiring storage to the SAN storage solution.

We will refresh the EMC Centera for the immutable storage tier in the Tulsa data center and at the DR site. The immutable storage is replicated from the Tulsa data center to the DR site to ensure a copy of the documents on immutable storage are available during a DR event.

At the document processing center (DPC) Tier, we will use a storage cache for scanned paper documents that will be transferred to immutable storage in Tulsa.

Rationale: Tiering Level. The current 3PAR P10000 arrays in Tulsa and Plano use 15,000 RPM drives and 7,200 RPM drives. In the current configuration, the drives in use include:

- Tier 1 storage of 15,000 RPM drives thickly provisioned and the highest performing RAID levels

- Tier 2 storage volumes consist of:
  - 15,000 RPM drives that are thinly provisioned
  - 15,000 RPM drives that are configured using a low performance RAID level or storage volumes containing 15,000 RPM and 7200 RPM drives.
- Archive Tier storage volumes created from only 7200 RPM drives.

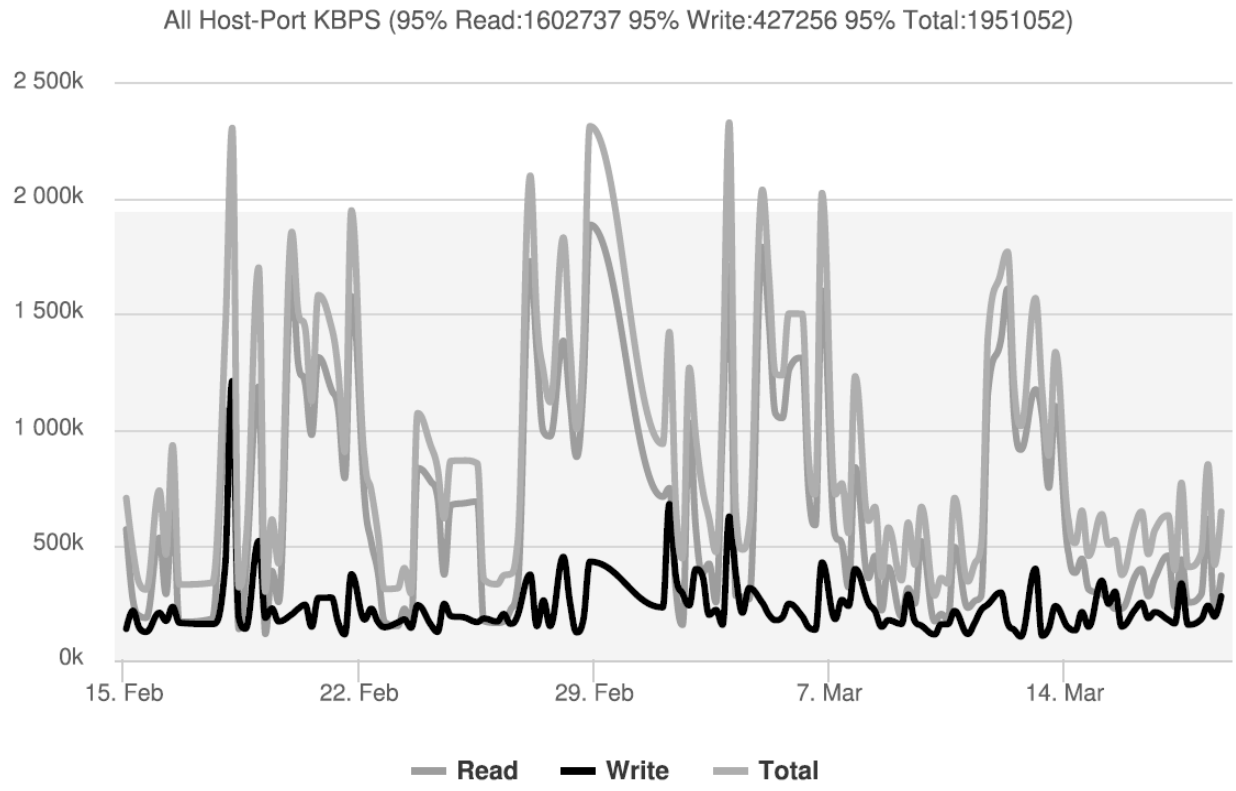
The storage solution provided is a 3PAR 20000 with the same storage tiers provided from 10,000 RPM drives and 7,200 RPM instead of the 15,000 RPM and 7,200 RPM drives. This is possible because the new 3PAR 20000 uses an internal infrastructure to achieve better performance using 10,000 RPM drives. The architecture features the HPE 3PAR Gen5 Thin Express ASIC for hardware accelerated thin technologies, including inline deduplication and 5.6TB of flash storage. Using 10,000 RPM drives provides a lower price per GB of storage at a higher level of performance.

The 3PAR 20000 solution with SSD disk drives, 10,000 RPM disk drives, and 7200 RPM disk drives was selected to provide better performance with lower cost disk drives than the current 3PAR P10000 with 15,000 RPM and 7200 RPM drives.

The current 3PAR P10000 storage is using a maximum throughput of only 2450 KBs per second, and the proposed 3PAR 20000 with 10,000 RPM drives is able to provide throughput of 2438 MBs per second—a rate that is nearly 1,000 times greater than the County is using in their current storage solution.

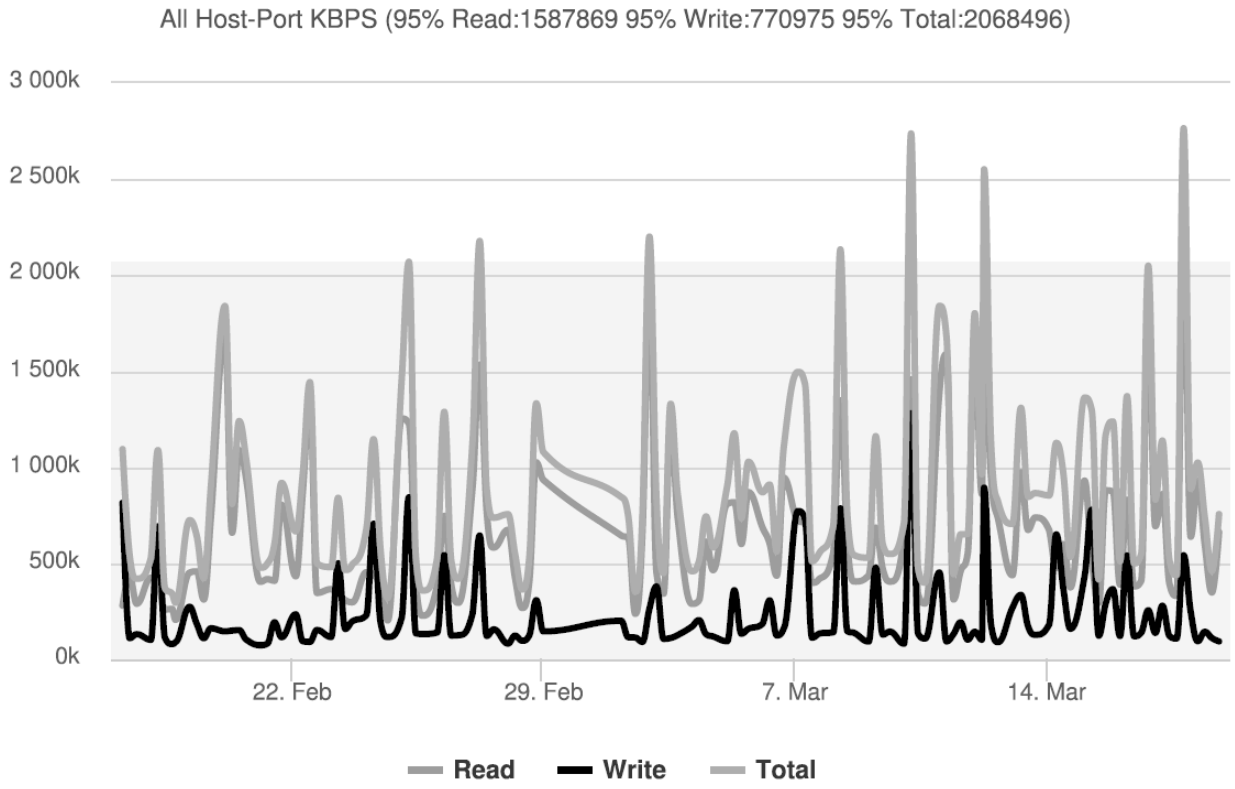
Figure 113. (Tulsa) and Figure 114. (Plano) were generated from the County's recent storage activity. Performance data from the two current 3PARs were used to simulate the expected performance of the new frame. The current Tulsa and Plano 3PAR P10000 reached a peak of ~2450 KBs per second, while the 3PAR 20000 10000 RPM drive storage is capable of 2438 MBs per second. The 3PAR 20000 is the latest innovation in enterprise storage from HPE. It is the evolution of the time-tested 3PAR storage, so there is little risk to the County by refreshing this storage. Primary data (all 3PAR-based tiers) is replicated to the DR site for applications requiring a 48-hour RTO. Figure 115 summarizes performance of 3PAR 20000 with 10000 RMP drives.

Figure 113. Tulsa 3 PAR P10000 KB per second, Feb. 18, 2016 to March 14, 2016



These types of reports help HPES to continually monitor storage usage compared to storage capacity.

Figure 114. Plano 3PAR P10000 KB per second, Feb. 18, 2016 to March 14, 2016



This report demonstrates that the County has sufficient storage capacity to meet its peak needs.

Figure 115. Performance Summary 3PAR 20000 with 10000 RMP Drives

Drives	Qty	Model	RAID	Workload	I/O size	R/W	MB/S	IOPs
SAS	608	1.2TB SAS 10K SFF	RAID5 (7+1)	Random	32K	60% Read	2,438	30
SSD	32	400GB SSD SFF	RAID5 (3+1)	Random	32K	50% Read	4,712	150,796

EMC Centera was chosen for immutable storage. EMC professional services will be used to install, configure, and migrate the existing immutable storage environment to the refreshed environment.

HPES selected this storage solution because it delivers a cost effective approach through the use of different types of storage media aligned to meet the criticality of the applications being stored. In combination with the MPC storage capabilities, the storage capacity provides the flexibility desired by the County because it can be allocated as needed to meet changing requirements.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

With consolidation of the data centers to Tulsa, storage will be provided at Tulsa and at the DR site in Colorado Springs, with replication as described above. HPES will provide storage administrators in Tulsa and a supplemental staff in San Diego to support all County locations in the area. All of these sites are access controlled, to restrict physical access only to people who need it.

Our San Diego storage team has overall storage management responsibilities as the central storage management point for the County.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES follows established and proven methodologies and key process in all aspects of operations and maintenance (O&M) support and we will continue to fully support the County as described below.

- We will utilize an ITIL framework, our proven SOPs, industry standard best practices and County policies, processes and procedures to provide storage and innovative, proactive, and responsive O&M.
- Work with the County to develop plans to migrate service from direct attached storage to SAN storage.
- Refresh, support, and manage DPC storage.
- Work with the County to make sure application infrastructure services us SAN storage.
- Support the traditional data center and MPC in Tulsa using the same SAN 3PAR to provide a centralized storage services solution managed by a single SAN administration team.
- Provide usable capacity reports to the County not to include replicated, backup, or DR data storage.
- Provide 20% year-over-year storage growth for 5 years to accommodate the County's business growth.
- Produce storage services reports by storage tier to the Business Group, department, and end-user levels.
- Provide OneDrive for Business for user unstructured data storage on Microsoft's Government Community Cloud. User can log into the OneDrive for Business portal to monitor and self-manage OneDrive storage. HPES will work with the County to provide self-service reporting and self-service management in other areas of storage services. Initially this will be access to regular monthly storage reports via the Service Portal, but if desired, we can expand this to include ad-hoc reporting
- Work with the County to lower the cost of storage.
- Continually evaluate, evolve, and deliver plans to reduce data loss for storage services.
- Produce and submit recommendations on storage services architecture.
- Produce and submit plans on shared storage services consolidation and application server migration to shared storage services environment annually.
- Produce and submit storage services policies and procedures.
- Produce and submit storage services reporting policies and procedures.
- Produce and submit storage services refresh plan annually.
- Produce and submit plans for meeting storage demands.
- Produce recommendations for process improvement in backup and recovery for storage services assets.
- Recommend and submit recovery policies/procedures for storage services assets.
- Produce and submit recommendation on capacity management.
- Produce and submit plans to add storage.
- Plan and schedule all storage-related software/driver/microcode patching and upgrades.
- Design and implement recovery processes based on approved policies/procedures.
- Design and implement storage services management processes based on approved policies and procedures.
- Implement storage services reporting.
- Design and implement storage consolidation based on approved recommendations.
- Deploy, manage, communicate, and report on activities related to storage service refresh
- Design and implement storage services provisioning and allocation processes based on approved policies
- Design and implement capacity management
- Implement approved Storage services policies and procedures
- Implement necessary physical and logical security to protect the County's data (through access controls, storage network, and host-based allocation controls, SAN zoning and host/array-level logical unit [LUN] masking).
- Provide support, including break-fix, for all storage services assets.

- Manage and affect the appropriate resolution of Incident events until the operation of the storage is returned to normal by following customized procedures as well as resolving Incidents upon an automated or manual detection of an event related to storage components
- Manage and support the storage services,
- Produce and submit monthly storage services reports,
- Support storage services refresh,
- Perform and support media management activities for storage services
- Manage and support the media requests
- Provide data storage services (such as RAID groups, storage pools, LUNs, presenting— masking and zoning, reclamation, optimization—tiers, deduplication, thin provisioning, among others)
- Perform tapes mounts as required.
- Perform special tape shipments as requested.
- Provide options for on premise and offsite data backup storage.
- Provide backup and restore options such as single user restore.
- Load and manage third-party media as required.
- Prepare and manage media for use by microfiche service.
- Manage and perform file transfers and other data movement activities related to break/fix or consolidation of storage services assets.
- Perform data backups of storage services per approved policies and procedures.
- Perform recovery processes on storage services assets.
- Perform storage utilization management.
- Manage and maintain all storage services assets and services.
- Produce and submit storage services management reports,

- Automated Tools – Automated systems and tools involved in proposed solution

HPES will use tools native to 3PAR that are included in the software of the storage devices.

The 3PAR provided in this solution is capable of creating thinly provisioned volumes. The HPES storage team is well-versed in managing these volumes, including close monitoring of volume growth that results in having storage available when needed. Traditional provisioning of storage volumes generally results in large amounts of unused storage that has already been dedicated to a host. Thin provisioning allows for over allocation of the 3PAR storage array and reduces the County's cost by delaying physical storage increases.

The 3PAR also has auto tiering capabilities with flexible configuration rules that allow for internal automatic migration, lightly accessed data on high performance, high cost storage to more cost effective, lower performing storage when the need for high performance storage is not warranted, based on the auto tiering configuration. The auto tiering configuration is flexible and allows HPES to adjust the data migration criteria to rebalance data and free up higher performance storage as needed.

HPE 3PAR System Reporter Software will be used to automatically collect data on a number of different object data points in the background. The Storage Administrator will use the 3PAR StoreServ Management Console (SSMC) or the 3PAR Command Line Interface (CLI) to display and report on collected data from an array. Using the SSMC, graphical reports are available for the following metrics.

• Historical data (Performance, Histogram, Capacity)

• Real time data (Performance)

HPE 3PAR System Reporter is a feature-rich analytical engine, which will help Contractor interpret and respond to collected performance data and make sure the Portfolio Applications are performing optimally in the environment.

- Qualifications and Experience – Background and experience in comparable environments

County of San Diego: HPES provides secure off-site storage for designated media, transporting media to off-site locations as required. Off-site facilities have complete fire protection and multiple layers of physical security to prevent unauthorized access.

HPES provides the County with a managed storage services (MSS) utility model with departmental storage on-demand services. This provides predictable price and performance levels for three types of storage: storage area network (SAN), network attached storage (NAS), and direct-attached storage (DAS). The current hosted storage capacity for SAN and DAS is 1200 TB, which includes 1,000 servers and 3,500 disks/tapes. NAS is attached at the desktop level and broken into 30 TB of Tier 1 storage (mission critical information) and 22 TB of Tier III storage (long-term retention). The tiered storage provides cost benefit to the County because Tier 3 storage can be leveraged at a substantially lower cost due to its availability and recovery time, and the County only pays for storage as they need it. HPES provides daily data forecasting to identify additional storage resources as needed.

U.S Navy Marine Corps Intranet (NMCI): Since 2005, HPES' experienced team managed and monitored a diverse SAN environment that consisted of two vendor's SANs. Recently, the team has designed, engineered, and implemented a one-platform SAN environment to standardize NMCI on the more flexible, ease of use and support NetApp SANs. Our team replaced all the non-NetApp storage to achieve a single-vendor SAN environment with a single set of tools, reports, and storage-allocation techniques. This single-SAN approach allows us to capitalize on native capabilities to provide site-to-site resiliency and reduce backup overhead through a storage hub and tapeless backup. Our single-SAN design reduces complexity and total operating cost (TOC) while increasing operating efficiencies and effectiveness. Our NMCI storage engineering team includes five technology consultants who have 35 years of combined experience on NMCI. Additionally, an imbedded systems engineer from NetApp augments our staff. We currently manage approximately 5 petabytes (PB) of NetApp storage deployed to more than 20 server farms.

A recent upgrade in storage technology opened up 300 TB of space and enabled NMCI administrators to more efficiently manage, store, back up, and protect information on the network. The upgrade also improves Navy Marine Corps storage scalability in preparation for an anticipated increase in information demand.

Defense Health Agency: HPES' system administration team currently supports more than 1,400 hardware components, 3,075 virtual servers, and more than 480 TB of storage hosting 12 applications on the MHS Application Access Gateways (MAAGs) located at 19 Military Treatment Facilities (MTFs) around the globe.

HPES also provides engineering support for HPES EVA 6500 and EMC CX300/320/500 SANs with a combined raw storage capability of 866 TB worldwide.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Backup and Recovery Services (Sched. 4.3, Section 6.13)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Backup and recovery (BUR) services play a key role in maintaining the reliability and resiliancy of the County's IT infrastructure, should problems arise. HPES will continue to create backup schedules and policies for the County's data. Implementing proven technology solutions to deliver efficient and effective BUR services, coupled with well-defined processes that are consistently executed, help the County meet its desired service levels. We will continue to monitor the backup infrastructure, follow the change management process, facilitate backup completion within our scope of control, and restore backup data on a consistent bases by performing backup restore tests at least once per quarter. Further, with plans underway to consolidate consolidate the services currently distributed between the Plano and Tulsa data centers, the BUR solution must be adaptable to a non-disruptive transition of services.

HPES will continue to provide the current BUR services at the Plano and Tulsa data centers, and at the County's document processing centers, which have proven to be effective during the past 10 years.

In preparation for the data center consolidation, HPES will collaborate with the County to provide planning support and minimize disruption as workloads and technolgies evolve while providing O&M support during transition without interruption.

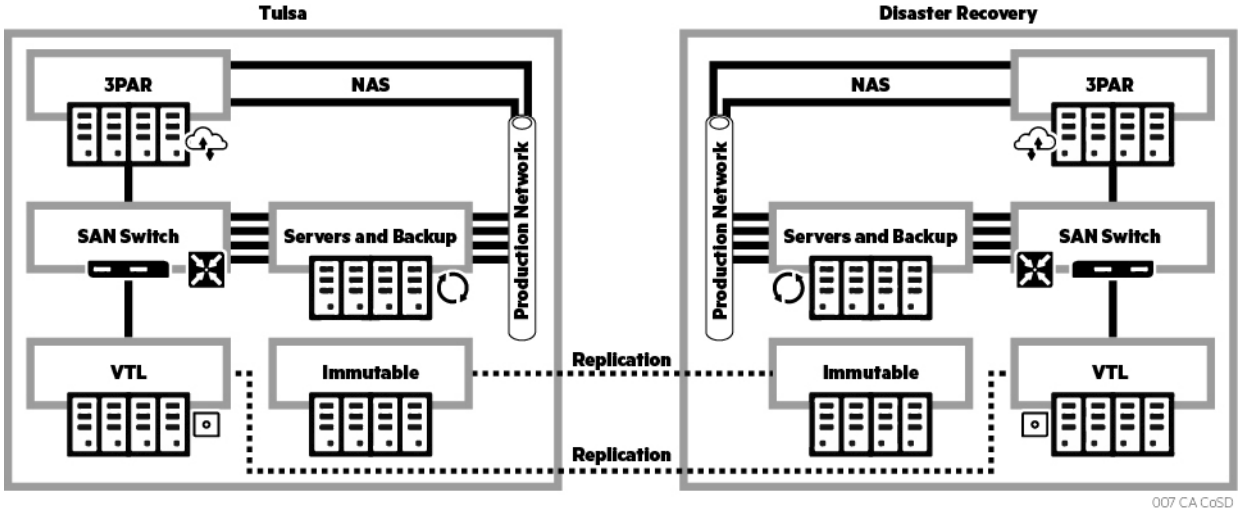
The existing production backup sets will be copied to the new solution so that no backup set data is lost during transition. A StoreOnce VTLat the DR site will join the backup environment as a replication target. Backups will be replicated to the DR site. Full replication of backups serves two purposes:

- For applications that require a 72-hour or greater RTO for DR, these backups will be used to restore service at the DR site.
- For all applications, the duplicate backup system provides restore capabilities in the event the primary system is unavailable for an extended period of time. Since this scenario is unlikely, leveraging the backup system at the DR site for this purpose is more cost-effective than having both a High-Availability system in Tulsa and replicating a subset of data for DR.

As services are migrated from Plano to Tulsa, our backup administration team will create the service's schedule and policy in Tulsa and remove the service backup schedule and policy in Plano. These backup sets will be replicated to the DR site as they are created. When all Plano service are successsfully migrated to Tulsa, the backup environment in Plano will be decommissioned.

After consolidation, HPES will provide the County with reliable BUR services and meet the requirement for off-site storage. Our solution incorporates 100% duplication of BUR data for the production data center at the DR site. The information will be replicated between the sites using a dedicated network connection. The backup sets will be stored in a Virtual Tape Library (VTL) at both locations. Figure 116. illustrates this solution.

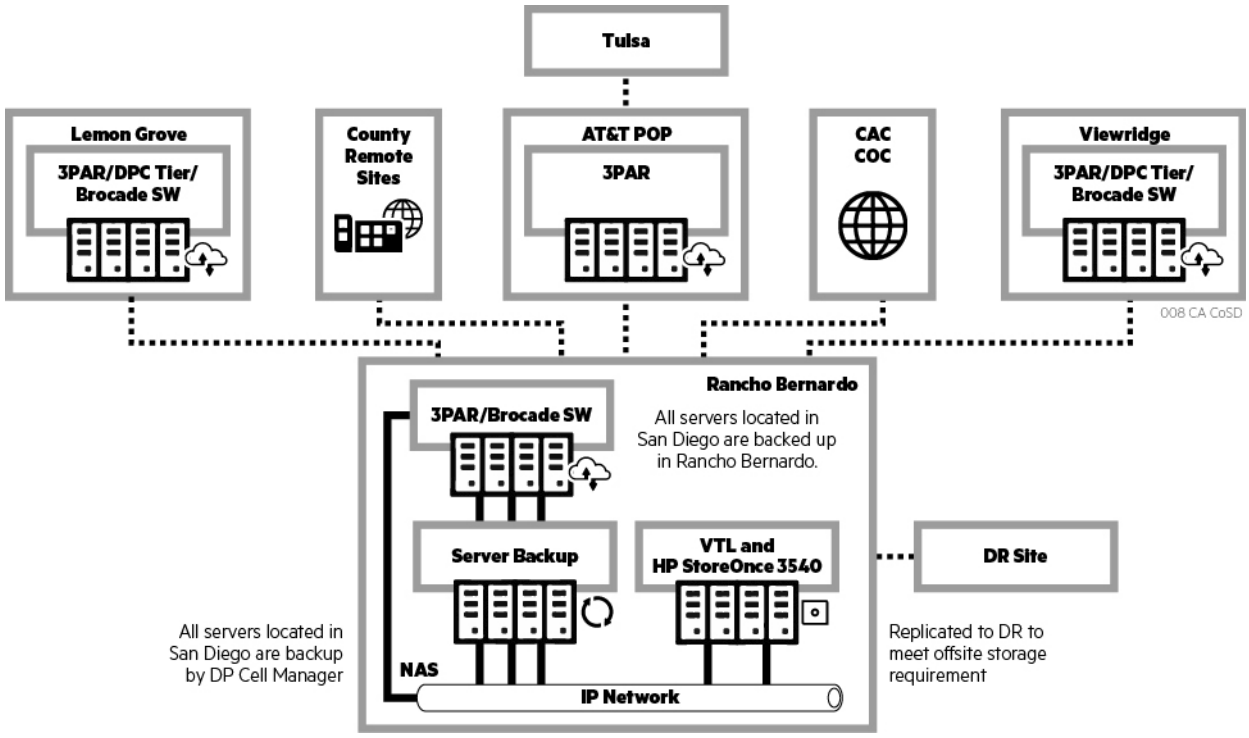
Figure 116. Future Logical View of Data Center Mid-range Server Storage / BUR



HPES' BUR solution provides 100% redundancy of backups in the Tulsa data center and the DR site, providing secure off-site storage of backup data, improved reliability, and quicker data recovery.

In the County's document processing centers, HPES will create and consolidate backups in Rancho Bernardo using a small disk-based VTL, which will be refreshed with a replacement of similar size. These backup sets will also be replicated at the DR site in Colorado Springs. Figure 117. provides an overview of this solution.

Figure 117. Future Logical View of Document Processing Centers Storage / BUR



HPES' BUR solution for the data processing centers provides added reliability by backing up servers to Rancho Bernardo and replicating those backups for off-site storage at Colorado Springs.

HPES performs backups of the AT&T POP, Lemon Grove, Viewridge and Rancho Bernardo (collectively known as the San Diego sites) in Rancho Bernardo. We will copy the existing Rancho Bernardo backup data sets to the replacement VTL to prevent backup dataset loss during the refresh. During the transition period, we will also replicate the Rancho Bernardo backups to the DR site for off-site retention. This approach provides several advantages:

- Elminates the need for a physical tape library and physical backup tapes, reducing the time required and complexity associated with performing backups.
- Eliminates the need to transport tapes for off-site storage by taking advantage of the DR site to perform this storage function.
- Speeds data restore activities by eliminating the time required to obtain backup tapes from a remote storage facility.

Industry Analyst Comments on HPE Data Protector

- **Gartner:** HP[E] was early in delivering snapshot integration and automation…which support HPES, EMC, and NetApp storage array snapshot and replication.
- **Forrester:** HP[E] Backup and Recovery appears to be heading in the right direction, with a focus on transparency, customer satisfaction, and delivering "HP on HP."

When the data center consolidation is complete, the production and Dev/Test, storage and BUR infrastructure, and O&M support will be provided in Tulsa, with DR capabilities in Colorado Springs, Colorado. The HPES backup administratiom team will continue to provide centralized backup and recovery management from any location because all backup will be to VTLs and replicated to the DR site over a dedicated replication network connection, eliminating any local tape handling requirements. All County data will be backed up, as required.

Built on HPE Data Protector 9.0 software, HPES' BUR solution will provide comprehensive functionality designed for enterprise environments using a dynamic and agile data protection strategy. HPE Data Protector servers will integrate with LDAP authentication services and support file inclusion and exclusion as an extra level of control. The HPES administration team provides for auto-discovery of virtual servers, supports single-pass image backups of virtual servers, provides integration of HPE Data Protector with Oracle RMAN, and integrates with VSS to backup Shadow copies that have been created. It will provide standardized backup and recovery across applications, formats, storage platforms that include disk, snapshots, tape, and cloud, with improved reliability if it becomes necessary to load stored backup data in the event of a failure. It will provide standardized backup and recovery across applications, formats, storage platforms that include disk, snapshots, tape and cloud, with improved reliability if it becomes necessary to load stored backup data in the event of a failure. HPE Data Protector provides real-time operational intelligence through a customizable BUR dashboard, that we will publish on the Service Portal. Information available through the dashboard provides insights into key performance indicators of the backup and recovery process.

Backups will be weekly full backups and daily incremental backups. The backup retention period is customized within the policy that defines the backup, based on the type of data being backed up. Custom retention periods can be defined for specific Portfolio Applications, with County approval if the retention period requested is outside of the policy. HPES will categorize the types of data requiring backup and retention timeframes, as detailed in Table 57, when developing the BUR solution.

Table 57. Types of Data Requiring Backup and Retention Timeframes

TYPE OF DATA	RETENTION PERIOD
User unstructured Data (NAS): • H: Drives	90 days

TYPE OF DATA	RETENTION PERIOD
• S: Drives • Application Test/Dev • Application Production	
Exchange 2010 (Email) • All Passive databases	14 days
Structured Data (Databases) • Test/Dev • Production	30 days
Application Servers • Test/Dev • Production	30 days
Infrastructure Servers • Domain controllers, SCCM Servers, Citrix, among others	30 days
Immutable Storage • Host based backups	30 days

For the County, the hardware solution is comprised of:

- HPE Data Protector Servers (7 cell managers and 9 media managers)
  - Cell managers are the servers that control, monitor, and store all backup object information
  - Media manager servers connect to backup target medion (disks, virtual tape or physical tape media) to access those media destinations.
- HPE StoreOnce B6600 disk-based backup media target, or VTL, in Tulsa. All Tulsa data center backups are replicated to a VTL in the DR site in Colorado Springs
- HPES StoreOnce 3540 is also replicated to the DR site for off-site backup set protection.

Additional functionality provided by this solution includes the following:

- SharePoint – granular restore
- VM Server – snapshot restore
- Synchronized backup application for the Enterprise Document Processing Platform (EDPP).

For cloud applications hosted outside of the Contractor data center, backup options will be provided by the Cloud Service Provider.

Rationale: HPES selected this approach because it provides the capability to store 100% of backup data at both the production data center and the DR site. This will provide improved reliability by eliminating a point of failure present if portions of data are backed up by different sites, which is the current process with the Plano and Tulsa data centers.

The solution builds on the HPE Data Protection application currently in use and facilitates a smooth transition during data center consolidation activities.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Until the data center consolidation is complete, BUR services will continue to be provided in the Plano and Tulsa data centers and the County document processing centers at Lemon Grove, and Viewridge.

After the data center consolidation, which will be complete approximately 9 months after contract award, Tulsa will serve as the production data center and Colorado Springs will be the DR site. The County document processing centers at Lemon Grove and Viewridge will continue to serve the same functions as they do currently. At this time, the space provided for the County in the Plano data center will be released and connectivity from the AT&T POP will serve Tulsa only.

HPES will provide backup administrators in Tulsa with additional local staff to support the San Diego sites and be responsible for management of the immutable storage in Colorado Springs. They will also manage the replicated images, 100% of which will be replicated to the DR site.

SAN and SAN storage hardware will be managed by HPES USPS resources.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES has documented and proven BUR processes that we follow under the current contract for both daily and weekly backup activities. We perform daily backups from 6:00 p.m. PT – 6:00 a.m. PT and full weekly backups from 6:00 p.m. PT on Friday through 6:00 p.m. PT on Saturday.

These processes address the following types of backups:

- Virtual Servers – Snap Shot
- Every other server – Host-based
- NAS – Fiber Channel

Specific process documents are discussed in Table 58.

Table 58. Process Documents

PROCESS	PURPOSE
HPE Data Protector Backup Verification Process	This purpose of this document is to verify that backup data can be restored and read. This is performed weekly by the BUR Administrator.
Preparing HPE Data Protector Cell Managers Prior to Scheduled Backups	The purpose of this document is to outline the steps preparing HPE Data Protector Cell Managers prior to scheduled backups. This is performed weekly by the BUR Administrator.
Upgrading the DPA Collector Agent on HPE Data Protector Cell Managers	The purpose of this document is to outline the steps to upgrade the DPA collector agent on the HPE Data Protector cell manager servers. This is performed weekly by the BUR Administrator.
Restarting Stalled or Unresponsive HPE Data Protector Backup Sessions (DOC ID BUR 0010)	The purpose of this document is to provide the process to be followed when In-progress backup sessions appear under Monitor in the HPE Data Protector Manager GUI, but attempts to view the session result in the GUI freezing. This is performed as needed by the BUR Administrator.
StoreOnce Troubleshooting (DOC ID 0015)	Outline the process steps on how to troubleshoot the StoreOnce application. This is performed as needed by the BUR administrator
Workaround for Hung Sessions Due to Catalyst Media Server Timeout (DOC ID 0017)	Outline the steps and workaround procedures for hung sessions due to Catalyst media server timeouts. This is performed as needed by the BUR administrator.

PROCESS	PURPOSE
How to Restart and Resume County of San Diego Backup Sessions (DOC ID 0018)	Outline the steps for restart and resume County backup sessions once failed objects and sessions have completely failed. This is performed as needed by the BUR administrator.
How to Kill the HPDP Session Using PID with Catalyst Devices (DOC ID 0019)	The purpose of this document is to outline the process steps on how kill the HPDP session using PID with Catalyst devices. This is performed as needed by the BUR administrator.
How to Archive Bit Reset Configuration for SQL Flat Files in HPE Data Protector (DOC ID: 0020)	Outline the process steps on how to archive bit reset configuration for SQL flat files in HPE Data Protector. This is performed weekly by the BUR administrator.
Resolving Latency on User and Data Shares (DOC ID: 0021)	Outline the steps and procedures for resolving latency on user and data shares. This is performed weekly by the BUR administrator.

HPES has identified the following opportunities to implement continuous process improvements:

- Data classification requirements, described in Section 2.9.9, can affect the capacity of the storage hardware. As this evolves, we will improve the data storage to meet these requirements in a cost effective manner.
- Anticipate incrementing storage 20% year-over-year for first 5 years to accommodate growth in storage requirements.

- Automated Tools – Automated systems and tools involved in proposed solution

Table 59. Automated Tools

SYSTEM/TOOL	PURPOSE
BUR Dashboard	Takes the automated reporting from HPE Data Protector and presents it on a dashboard. This notifies BUR admins and end users of both successful and missed backups. This information identifies for the BUR admins which nodes to work on and troubleshoot. Once BUR jobs are configured, these are automated and run daily

- Qualifications and Experience – Background and experience in comparable environments

HPES currently performs all required BUR services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: HPES manages the County operations environment, which is a large, agency-wide environment that includes a modernization and virtualization, an operations service desk and data center environment, and a secure network environment. HPES is also responsible for complete backup, recovery, disaster mitigation support and system controls to monitor network access, system applications, data security, systems monitoring, end-user services, and support for continuity of operations services.

HPES upgraded the BUR solution by replacing the outdated Tivoli Storage Manager (TSM), which had reached end-of-support, with HPE Data Protector. This solution provides the ability to do fully weekly

backups and incremental backups during the week and store the information in a VTL, which significantly reduces the time and complexity to complete restore activities.

Virtual tapes are much faster than physical tapes from a media perspective, since these are a disk/disk array, which does not require swapping tapes in and out of a library. It also eliminates the possibility of defects/breakages in the tapes.

Following the upgrade to HPE Data Protector, one of the first server restores was completed in 20 minutes, compared to a minimum of 4 hours using TSM.

City of Anaheim: HPES provides operational support for data center operations that includes routine system operation functions and system console operations actions (for example, reboots), scheduled and ad hoc backups and restorations, batch operations (such as automated and manual batch scheduling and monitoring), capacity monitoring and planning, and performance management (such as monitoring and reporting). We respond to all manual and automated tape mount requests and work to maintain the integrity of the tape media environment.

HPES supports a Microsoft-based network for the City. We perform modifications, enhancements, changes or other maintenance necessary to correct errors such that each item of database software operates according to its applicable specifications and to any applicable service levels; performs database space management, capacity planning, and performance tuning functions; and performs disk load balancing (moving data from one file system to another as a result of capacity constraints or performance problems).

Some of the projects that we have completed to expand network capabilities or to enhance network efficiency include:

- Implemented WAN/LAN network enhancements to provide improved uptime, reliability, and security.
- Installed an outdoor wireless network using a licensed bandwidth dedicated to public safety.
- Implemented new backup systems with improved backup, restore, and response times.
- Expanded the storage solution for records retention.

Commonwealth of Pennsylvania Data Center Computing Services: HPES installs, allocates, and manages storage, and performs all storage administration tasks, including BUR and archiving. We have used automation to a large degree to automate many of the allocation tasks, significantly reducing the time and errors associated with provisioning.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Managed Print Services (Sched. 4.3, Section 6.14)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The County's high volume and diverse managed print requirements necessitate a reliable hardware and software solution coupled with formalized processes, described below in the Methodologies and Key

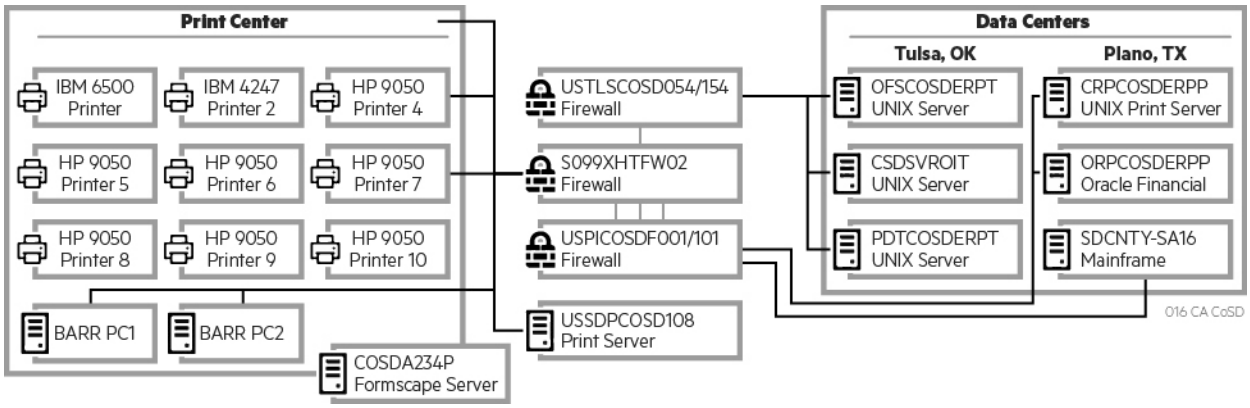
Processes section to facilitate timely and consistent report production and delivery to multiple agencies throughout the County.

Since 2010, HPES has provided managed print services via the County print room facilities located in Rancho Bernardo. Our print operations processing takes place Sunday through Friday from 8:30 p.m. to 2:00 p.m. PT, with on-call support available as needed. There are two kinds of print requirements specified in the RFP. We currently provide and address each in the appropriate section. Managed Print Services, also known as Print Center or Print Services is described in this section of the proposal. The other requirement is for Network Print. There are the printers attached to the LAN used by users and managed under the end-user services RU as described in Section 2.7 of this proposal in response to Schedule 4.3, Section 4.11).

Recognizing there are a number of changes occurring in the environment, such as a transition of managed print services for Juris requirements to another vendor, consolidation of the data centers to a single production center in Tulsa, and migration from the SA16 LPAR Mainframe and A/S400, HPES' solution easily accommodates the changes.

With the transition of the Juris-managed print requirements to Fujitsu, HPES will continue to provide managed print services of approximately 200,000 pages per month on average to meet Assessor and Tax Collector requirements. This will be conducted at our print facilities in Rancho Bernardo. HPES will use the BARR print management tool to receive the files for printing. Figure 118 illustrates how print files are currently transmitted to HPES' print center.

Figure 118. Transmission of Print Files to Required Printers



The HPES print center is equipped with a variety of printers to efficiently meet the County's unique print requirements and print volumes.

Migration from SA16 LPAR Mainframe to the Integrated Property Tax System (IPTS) will consolidate and modernize the legacy property tax systems in a web-based system designed to vastly improve the efficiency of the property tax-collecting process. It will also generate the tax bill files for printing. We are currently testing new file formats to validate compatibility with existing printers as these will remain in place. After implementation of IPTS, HPES will update processes and procedures associated with running daily print jobs for County Assessors and Tax Collectors.

HPES will continue to provide the following services for the managed print framework component:

- Order supplies such as HPES print toner and printer maintenance kits
- Ordering special forms and paper
- Provide support for microfiche
- Daily delivery of approximately 12,000 pages of reports to:

- County Operations Center Drop with delivery no later than 06:00 a.m. PT on Monday, Tuesday, Wednesday, Thursday, and Friday
- Sheriff Marshall's data center and Ruffin Road Annex with delivery no later than 07:30 a.m. PT on Monday, Tuesday, Wednesday, Thursday, and Friday
- On-call support from HPES is available daily until 2:00 p.m. to print and deliver to any of the regular drop locations.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Our primary print facility will be the HPES location in Rancho Bernardo and with the implementation of a disaster recovery solution, multiple geographically diverse sites have the capability to provide print services for the County, facilitating uninterrupted print business operations should a disaster strike (for example, wild fire or earthquake). Print jobs will be easily routed to any location. Table 60. summarizes the specific types of printing provided at each location.

Table 60. Types Printing Provided at Each Location by HPES

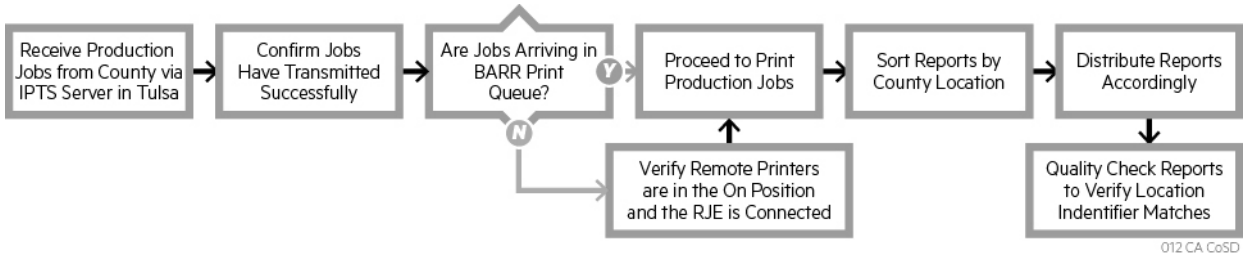
TYPE OF PRINTING	LOCATION
Laser and Impact Print	Rancho Bernardo
Annual tax bills, supplemental (small volume) tax bills, and tax bills that require manual intervention of the Treasurer-Tax Collector's (TTC) office.	Rancho Bernardo, with backup at Rancho Cordova
One-stop document and tax bill management—folding, envelope stuffing, and mailing	Rancho Cordova
Laser Print and Tax Bills (Dev/Test)	Troy, Michigan (trial) Rancho Bernardo Rancho Cordova

HPES' dedicated staff will work in the print center in Rancho Bernardo with responsibility for printing, distribution, and delivery of daily work.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

HPES adheres to established processes that enable us to attain the service level required by the County. Figure 119. illustrates the process followed by our staff to receive print requests and print the reports for distribution to the County within the prescribed timeframe in Service Level ID 39.

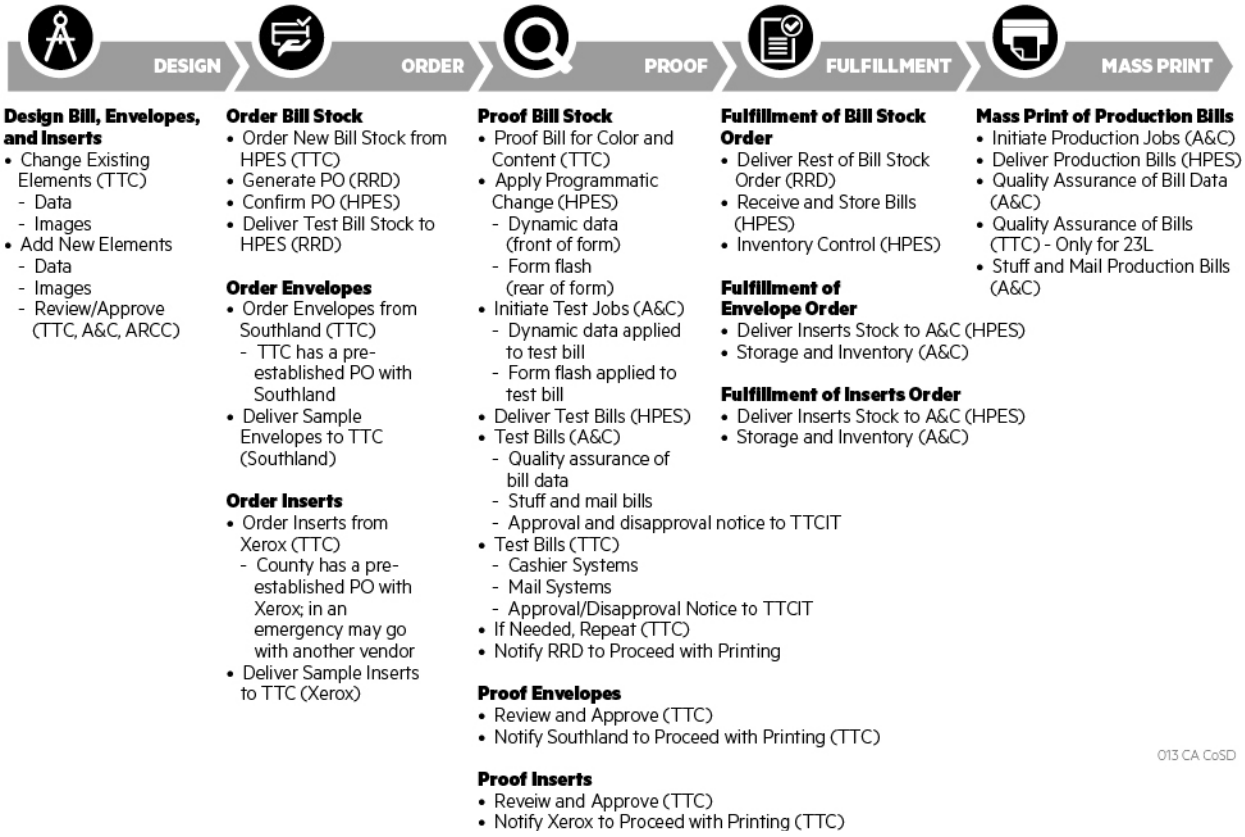
Figure 119. HPES Process for Receiving and Printing Reports



HPES' standard process makes sure that print jobs are completed and delivered to County locations in a timely manner to meet the required delivery timeframes.

Recognizing that tax bill generation is very complex and accuracy is critical, HPES, in collaboration with the County, devised a process checklist, shown in Figure 120 that our staff follows and has proven successful under the current contract.

Figure 120. Tax Bill Generation Process



Developed jointly between the County and HPES, adherence to this process makes certain that annual tax bills are printed accurately and on time.

HPES implemented several process improvements under the current contract that include:

- Created print to PDF solution alternative to reduce paper consumption along with the capability to send electronic copies of reports when requested by County. This improves the efficiency of County users who no longer have to wait until next the day for a hardcopy. This allows the print center to send a PDF document of a requested report within a few minutes of the request.
- Improved the alignment of annual tax bill print form to save print time, which resulted in improved quality of the 1 million tax bills printed. Typical print time for the bills to be printed during the past 3-4 years was 9-10 days. The 2015 print season was completed and delivered in 6 days.
- Through the course of the contract, HPES has achieved year after year process improvements when printing the SD County annual tax bills every September. There are typically 1-1.2 million tax bills that we print and deliver in a two week timeframe HPES has taken the initiative to reduce the time it takes to print and deliver the bills by working closely with the applications team to improve the job coding, allowing for better quality alignment with the tax bill form, reducing the extra time it takes to reprint a poorly aligned form. Two years ago we completed the bills and delivered these in 10 days; last year were completed the job in nine days and plans are underway to continue to improve the process to further reduce the time in 2016.

Additional potential process improvements include:

- Print to PDF capability to eliminate hardcopy
- Store items in batch from IPTS on SharePoint for a specified period of time
- Print to PDF at various County locations, making sure business units have access to the information they need to perform their work

- Automated Tools – Automated systems and tools involved in proposed solution

HPES uses the BARR Systems Print Server to automate and control print and document output.

- Qualifications and Experience – Background and experience in comparable environments

HPES currently performs all required managed print services for the County under the existing contract. Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

County of San Diego: HPES, at our print facility, prints a majority of reports required by Treasure Tax Collector, Property Tax Services, Assessors Office, San Diego County Courts (Vista, El Cajon, South Bay, SD Superior and Kearny Mesa Traffic). Some reports are distributed to the County for internal use, some are sent to County residents, and others are used in County court cases. Each department has special print jobs that are run daily, weekly, monthly, or annually and are transmitted directly to the print center via the County SA16 LPAR mainframe. The reports are then converted to a printable language, which allows the print operators to send these to various printers at the print center. We receive reports such as, tax bills, penalty warning statements, roll corrections, court subpoenas, legal dockets, traffic court convelopes, among others. The printing occurs overnight and reports are distributed to their designated locations in the morning.

Centers for Disease Control: HPES manages hundreds of file shares and print servers in support of CDC's more than 17,000 users throughout the U.S.

Airbus Helicopter: HPES provides a full-managed print services solution to offices in France and Germany. This support includes:

- Onsite services (with dedicated technical consultants for the company)
- Cartridge renewals
- VIP support (4-hour agreed service time)

In France, 70% of Airbus Helicopter's printing fleet has been replaced with HPES printing units. In Germany we have replaced 50% of the fleet. The printing units range from laser jet printers to large format printing units and include a total of 1,354 printing devices.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

Public Key Infrastructure Services (Sched. 4.3, Section 6.15)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

In late 2014, in coordination with the County, HPES initiated a project to implement the Symantec Managed Public Key Infrastructure solution after evaluations of various vendor solutions. Solutions were evaluated and scored per the County's vendor evaluation process and included Symantec, Entrust and ARX/Cosign. ARX/CoSign was eliminated since it was not a managed PKI solution. Symantec's solution was the highest rated product and was selected for use by the County. HPES will leverage the current MPKI 8.13 solution and use that as the foundation for additional PKI services, thereby preserving the County's investment. This solution is a fully extensible and redundant platform and is sized for the current project as well as future functionality. Key features and benefits of the Managed Symantec PKI solution are:

Key Features

- **Trusted, Cloud-Based Infrastructure:** Monitors, manages, and escalates across the globe with full DR and is certified as part of a SAS-70 security, WebTrust and specialized Government audits.
- **Broad Application Support:** Issuance of X.509 certificates that interoperate with operating systems, devices, VPN, mail, and web browser software. Certificate profiles for common applications are for email encryption and signing, and Adobe PDF signing.
- **Automated Certificate Life Cycle Management:** Automates configuration of authentication, encryption, and signing applications across platforms and browsers. Managed PKI service can automatically configure a user's browser, VPN client, mail client, or other application to use certificates. PKI Client also automates renewing certificates and prevents expired certificates from interrupting business continuity.
- **Enterprise Integration:** Integrate Managed PKI Service with a corporate directory to populate certificate meta-data, select and enforce certificate and application policies, and publish issued certificates. PKI Enterprise Gateway functions as a local registration authority integrating with hardware security modules to protect key material.

Key Benefits

- **Reduces PKI Cost and Complexity:** Managed PKI service's cloud-based approach dramatically lowers cost and complexity by eliminating the facilities, hardware, software, personnel, training, and maintenance expenses associated with deploying traditional in-house PKIs.
- **Simplifies the Administrator and End-User Experience:** Eliminates administrator tasks, and automates the process of provisioning certificates and configuring applications to use those certificates.
- **Maximizes Deployment Flexibility:** Not only can organizations deliver multiple certificate-based security applications from a unified platform, but they can also tailor the deployment to meet their needs.
- **Delivers Proven, Scalable, Reliable PKI:** Symantec's procedures, policies, and infrastructure have been proven with large enterprises, governments, and manufacturers around the world

Self-service via the proposed Service Portal, described in response to the Service Desk (Sched 4.3, Section 3.1), will be made available for specific use cases for optional services or functions, such as certificates required for digital signing of expense reports.

The approved County solution for digital signing is the existing ARX/CoSign document. HPES will work with ARX/CoSign to develop and implement previously identified changes in the document signing solution to utilize the Symantec PKI certificates as part of transition.

HPES will integrate Symantec PKI with DocuSign CoSign. Currently the internal CoSign CA is used to generate and revoke certificates. This will be replaced by a web service invocation to Symantec Cloud-

based PKI. Today the enrollment process automatically occurs when a County user on a County machine attempts to sign a document or open any application that uses the CoSign client plugin (e.g., Word, Excel, Adobe Reader/Acrobat). This process will remain unchanged. During the enrollment process, the CoSign appliances will invoke a web service against the Symantec Cloud-based PKI to fulfill the certificate creation request. Once complete, the private key of the certificate will be stored in the appliances' internal store (as is done today). Subsequent requests to sign documents will be fulfilled by the appliances only with no need to invoke Symantec services. This approach has already been successfully developed and deployed between CoSign and Comodo with production use by a number of customers. In addition to firmware changes, CoSign will have to recertify their appliances if Federal Information Processing Standard (FIPS) compliance is required. Firewall rule changes at the County will need to be created to allow connectivity between the appliances (currently in the data center zone) and Symantec PKI cloud. No changes are anticipated for Symantec. Additionally, no changes should be required for the CoSign clients residing on County desktops/laptops.

HPES will support the PKI solution using a combination of HPES County-dedicated resources and HPES corporate resources as part of the Identity Access Management solution. The PKI will be supported per the Data Center support model as stated in Infrastructure Services (Sched 4.3, Section 6.8). PKI functionality will be supported by the local Security team and the HPES Identity Access Management team, which currently supports Active Directory and ADFS as well as other AD integrated solutions. Operational support functions include monitoring certificate status to identify when they should be revoked or renewed as well as administrative management of certificate profiles and users.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES staff will be located at the following sites to support the County. We will continue to work closely with the County CIO, CISO, CTO and supporting staff, facilitating a cohesive working environment that allows for direct communication, excellence in service and responsiveness, and direct access to the HPES team by the County for quick resolution of any issues. These sites are:

- Rancho Bernardo. Primary location of dedicated HPES staff specifically assigned to support the County. It includes centralized meeting space for engagements between the County and its contractors and HPES personnel, including security staff and HPES executives, and is the initial point of contact for the County. Test environments, training, and video conferencing are also housed at this site.
- HPES Tulsa Data Center. This is the core data center that will house the majority of the County IT infrastructure and delivery of core IT services as well as security services.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

Certificate Practice Statements (CPS) are legally binding agreements between the County and its entities where certificates are used. These documents state the terms and conditions associated with certificate use and typically come into play into the event of perceived misuse. As such, the County will need to define the CPS, and HPES will facilitate that process.

The development and review of use cases is critical to the expansion and continuous improvement of the solution. Use cases identify new opportunities for PKIs and are key inputs into the roadmap. As use cases are identified, such as expansion of the platform to include all County users and external County agencies, we will review these with the County for consideration and approval.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES will use the Symantec Management Console to provision and revoke certificates and configure applications to use those certificates, reporting, and administrative user management .services.

- Qualifications and Experience – Background and experience in comparable environments

Following are examples that demonstrate this experience supporting the County and other clients with comparable environments.

San Diego County: HPES currently supports the legacy internal Microsoft PKI solution as well as the new Symantec-managed PKI solution. HPES is in the process of implementing the first set of use cases for the Symantec managed PKI solution. The use cases include device certificates for approximately 3,000 laptops, wireless devices (IOS, Android, Windows) excluding BYOD and SSLVPN (IOS, Android).

Department of Defense (DoD): HPES generated, coordinated, and maintained PKI planning documents that describe the operational role and responsibilities that validate compliance with PKI policies for the DoD. As the liaison for Joint Task Force-Global Network Operations (JTF-GNO) and United States Cyber Command (USCYBERCOM), HPES formulated responses to external PKI RFIs that relate to overall access control and authentication issues, issues and questions, and requests for policy guidance and interpretation of the PKI-related CTOs. As a result, the Combatant Commands, Services, Defense agencies, and DoD field activities can now report compliance.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

2.9.1 Offeror Response to Data Center Services Specific Questions

2.9.1. Describe your rationale for your proposed Data Center location and solution as it relates to disaster recovery requirements.

With the County's services currently divided between data centers in Plano, and Tulsa, we selected Tulsa as the location for the consolidated production data center to minimize disruption and streamline transition activities. At this time, more than 50% of the County's workload is supported in Tulsa, so consolidating the data centers to this location minimizes the impact to applications by reducing the number of applications that must transition to a new environment. This approach also reduces the amount of coordination required to make sure transition activities align with other County projects and initiatives to minimize potential impact to in-flight projects.

- HP (now HPE) was named "Leader" by Forrester in each of its last four reports on the industry – "The Forrester Wave: Disaster Recovery Services Providers."
- HP (now HPE) was named "Strong Performer" by Forrester in its first report on Disaster Recovery-as-a-Service – "The Forrester Wave: Disaster Recovery-as-a-Service Providers," Q1 2014 (most recent report).

The HPES Continuity Services center in Colorado Springs, Colorado, is the designated disaster recovery (DR) site for the County. HPES' solution incorporates 100% redundancy of infrastructure, provided on a subscription basis, for applications that currently require a DR solution. Production data will be replicated from Tulsa to the DR site using a dedicated network connection, as described in Section 2.9 Storage Services (Sched. 4.3, Section 6.12) of this proposal and illustrated in Figure 99 within that section. Our Colorado Springs center is a purpose-built, SSAE16-audited, world-class data center designed to meet the demanding needs of the modern computing environment. The Tier III design provides a concurrently maintainable and

continually operating facility with infrastructure built with redundant capacity components and multiple independent distribution paths serving the computer equipment.

We have designed a fully subscription-based solution that meets required recovery time objectives (RTOs) of 48 and 72 hours while also eliminating the current dual data center architecture. This approach is fully described in our response to Schedule 4.3 Section 2.17, Disaster Recovery Management Services. Note, however, that we recognize that the County currently has some applications designed as active/active for DR. By choosing Colorado Springs as the site for DR, we made sure that facility would have sufficient capacity to support a dedicated environment for an active/active architecture, should the County decide to reinstate it. We include in the new solution the core network components (Akamai and Global Traffic Management capabilities) to support an active/active architecture.

The DR location and solution provide recovery of production midrange and private cloud environments[2] as well as technical assistance for recovery of business processes. In case of a disaster, the production environment will recover gracefully in our Colorado Springs data center. Note that traditional VMWare and MPC environments are handled identically for DR purposes: the Managed Private Cloud is a collection of virtual servers, some of which will have DR recovery time objectives, some will not. The DR environments for the virtuals within the MPC will be virtual servers that spin up with a copy of the MPC virtuals, for those servers that have designated RTOs in Apps Manager. HPES selected Colorado Springs as the DR site based on the following features:

- It exceeds Tier 3 data center specifications and:
  - Is on two different power girds
  - Has multiple points of entry for telecom and Internet access
  - Has multiple on premise power generators that are physically separated—in different rooms with fireproof walls—to make sure that, if there is a fire, we do not lose all of our generators.
- Colorado Springs, as one of our premier Continuity sites, provides subscription offerings and Continuity professionals who are trained and certified in Business Continuity disciplines. They will advance the County's Disaster Recovery strategy and testing methodologies to provide full assurance of application recovery that meets the County's requirements.

Our Rancho Bernardo environment will use replicated backup sets at the DR site in Colorado Springs to meet remote backup set storage requirements, as described in Section 2.9 in response to Schedule 4.3, Section 6.13.

2.9.2. Describe your proposed strategy to identify and eliminate single point failures with infrastructure and portfolio applications in Data Center Services.

Eliminating single points of failure is critical to help the County deliver a reliable and predictable infrastructure. Knowing the importance of this, HPES assesses redundancy as part of our design process to avoid single points of failure in the infrastructure and for high-availability (HA) P-1 and P-2 portfolio applications, taking into consideration the criticality of the application or infrastructure element. We build quality into the design process by conducting peer reviews so that changes or additions do not create single points of failure.

In the current environment, at the network level, HPES provides redundant switches in the data center and redundant circuits to the data center. The physical servers have redundant connections to the network and

[2] As of this submission, the plan is not to move Tulsa production applications into the private cloud; however there is no technical impediment to doing so. Therefore the information about how DR applies to MPC is only relevant if and when production applications are moved into the private cloud.

to the storage fabric. Physical servers are configured with redundant components such as redundant power supplies, which are plugged into separate power leads in server racks. Storage arrays have redundant components as well, such as redundant disks and power supplies, and have the ability to automatically notify our support teams when an alert is detected on the array. At the application layer, for business-critical applications, we incorporate redundant web servers and application servers that are load balanced on the F5s. Databases for business-critical applications have replication and/or clustering enabled.

For those applications hosted in the cloud, the Helion Managed Private Cloud (MPC) incorporates the tools necessary to continuously monitor server availability across the environment to maintain hardware, upgrade firmware, investigate outages, and perform corrective actions to restore hardware when necessary. Both the MPC and traditional VMware environments include spare physical servers that can take over the virtual server load in the event of loss of a physical server in the virtual farm.

For the County, HPES designed the MPC hybrid cloud to eliminate single points of failure and meet the service level (SL ID 51) for application availability.

HPES fully supports the plan to eliminate single points of failure. For applications that are unable to meet Service Level 51 without additional redundancy (in both the MPC and traditional environments), we will add the necessary redundant components upon approval by the County.

Protecting the County's data and systems is vital to HPES; therefore, we design, implement, and maintain County applications in alignment with County priorities for criticality and sensitivity to meet and exceed service levels. The Data Center Services solution for the County incorporates the following.

- **Facility Redundancy**: All key components are concurrently maintainable, as defined by the Uptime Institute for Tier III facilities, including N+1 data links, power, uninterruptible power supplies (UPS), and cooling as well as redundant network connectivity, power supply, and electrical—this contributes to the County's ability to achieve operational excellence.
- **IT Architecture Redundancy:** The MPC architecture is designed for hosting of enterprise-grade workloads that demand high levels of system availability and performance in x86 private clouds; this supports the County's goal to improve the reliability of the infrastructure by increasing redundancy and availability. Internally, HPES maintains a "system-level" service level objective (SLO) up to 99.95% availability for the entire Infrastructure as a Service (IaaS) stack. This includes maintaining the availability of the compute; storage; network; security; backup hardware and software, up to and including the operating system (OS); the Cloud Service Automation (CSA) software; and HPES facilities.

  Diverse applications share virtualized resource pools, so the operating environment automates high-availability policies to meet key performance indicators (KPIs). A resilient, converged infrastructure provides the right level of availability for each business application.

  To eliminate server failures, the majority of County traditional hosted applications run on VMware virtual machines (VMs). VMware HA automatically moves and restarts VMs on other VMware host servers in the County cluster in case of failure or planned maintenance.

  Applications that run in a Solaris operating environment will use server clustering technology to provide redundancy when needed. Oracle servers requiring high availability will be deployed in server clusters. If the primary server node fails, services will automatically fail over to the redundant node. Failover also can be invoked manually to support a planned outage. More specifically, HPES provides redundancy the Solaris environment in the following manner:

- Disk
  - OS disk (internal disk): primary/mirror/altboot on three separated disks

  - Application files (external disk array): hardware redundancy
- HBA: At least two host bus adapters (HBAs) per server using either MPXIO or Veritas DMP for multipathing
- Networking: At least two physical interfaces for production IP using IP network multipathing (IPMP) or link aggregation.
- Server hardware: at least 2 power supplies/ two CPU cores

  Private cloud and traditional hosted storage use HPE 3PAR enterprise storage designed for cloud environments. The storage hosts OS images, virtual snapshots, and application data. All OS images for virtual machines boot from the storage area network (SAN). This architecture enables the server image to be disassociated from the physical hardware, allowing the server image to move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover for improved availability.

- **Application High Availability**: We use the F5 BIG-IP Local Traffic Managers (LTMs) to provide the County application HA by load balancing applications across multiple VMs. For example, the County's SharePoint 2013 environment uses the F5s to load-balance the front-end and mid-tier application servers; we implemented the same strategy for the test environment.

  Single points of failure are eliminated at the database layer by using database clustering strategies such as Oracle RAC (e.g., for Oracle IDAM) and SQL Always-On (e.g., for SharePoint 2013).

- **Disaster Recovery**: To cover higher requirements for redundancy to handle RTO/RPO requirements on mission-critical applications that include P1 Apps – 48 hours with <= 28 hours of data loss and P2 Apps – 72 hours with <= 28 hours of data loss, and services during a declared disaster event, we integrated HPES Helion Continuity Services delivered through the Colorado Springs DR site.
- **Server Management and Monitoring**: We install, manage, and monitor the OS instance and the underlying virtual and physical server. We monitor server availability, maintain hardware, upgrade firmware, investigate outages, and perform corrective action to restore hardware when necessary. We also maintain the health of infrastructure assets included in the solution, including server, storage, backup, network, and other devices. HPES currently uses HPE Operations Manager (HPOM) and SiteScope to detect problems and send selected alerts to a centralized management server for specific business-critical applications for County business groups. Thresholds are set on events to indicate potential problems, so that support teams can respond to them in time to prevent outage incidents.
- **Special Scenarios: Multi-Facility Presence (active/active facility-level requirements).** Our solution does not include multiple primary data center architectures for specific applications, because the RFP requires consolidation to a single data center plus DR. However, we recognize that we have, at the County's direction, employed this type of architecture for specific environments, namely AEM and NetMotion. In the single data center model, the redundancy components described in the "IT Architecture Redundancy" bullet above will be applied to these applications to provide high availability. For example, the Netmotion environment today consists of a single application server and a single database server in each data center. Following the consolidation to Tulsa, this configuration will be replaced with two load-balanced application servers and two clustered database servers. This will provide automated failover within the Tulsa site – a more robust configuration than the manual failover configuration in place today.

  If the County wishes to return to a multiple-primary data center model for specific applications, we can locate specific servers at other sites. The location and cost of this approach will depend on the volume and design required.

2.9.3. Describe your proposed strategy and approach to design and support an all virtual infrastructure in the data center. Include a description of your proposed process to measure and correct capacity across servers, networks and storage in a virtual environment.

Over the past 10 years, HPES has worked with the County to identify opportunities to virtualize the infrastructure, with approximately 70% now supported in a virtual environment. Continued virtualization on a standardized platform will help to further reduce the number of servers needed, resulting in lower hardware, facility and energy costs. Virtualization also helps to maximize hardware because each server supports a sufficient number of virtual machines to increase its utilization from the typical 15% to as much as 80%.

Approach to Design and Support an All-Virtual Infrastructure: The MPC implementation for the County will serve as the platform to support an all-virtual environment, providing the bridge from a hybrid environment to an all-virtual environment when feasible. HPES' approach to move toward an all-virtual infrastructure is to initially retain existing applications in the traditional hosted environment until scheduled for refresh or application upgrade. At that time, HPES will collaborate with the County, performing a cost/benefit analysis to determine feasibility to migrate additional applications to the MPC environment. In this analysis, we take into consideration items such as level of County hardware investment, timeframe for application retirement, if any, and the level of effort for legacy applications to be re-architected to run in the MPC, if applicable.

The hybrid solution for the County enables creation and management of virtual and physical pools of servers, storage, backup, and networking resources using a common management layer. It provides a predefined, prebuilt, highly standardized infrastructure environment designed to meet the County's needs and incrementally add capacity to accommodate additional applications.

MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases. HPES as part of the solution design will incorporate the license considerations to manage costs with the expectation of no change in license costs increase based on the virtual solutions.

As part of the Data Center Consolidation transition design process, HPES shall make all reasonable efforts to optimize County software licensing costs. County software has a variety of licensing models such as site/enterprise, concurrent user, named user, module, managed budget, server, CPU, and core. Licenses based on server, CPU, and core present an opportunity for consolidation and license cost savings.

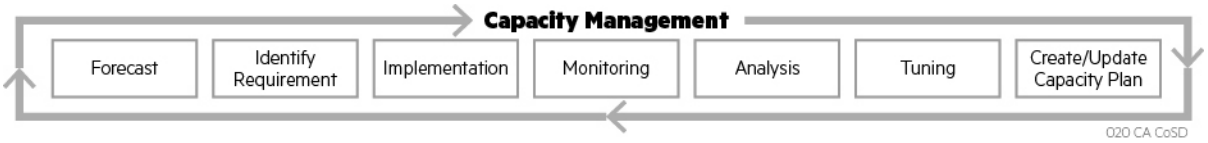
Methodologies to reduce license obligations for server/CPU/core based licenses shall include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated to headroom at each site versus single site's shared environment. HPES shall pursue these methodologies during the design phase of the Data Center Consolidation.

HPES leverages virtualization at the server, storage, and network levels to help the County increase the speed of business and deliver with agility. Virtualization separates the applications, data, and network connections from the underlying hardware, making it easy to quickly reallocate resources to match the changing performance, throughput, and capacity needs of individual applications. Through storage virtualization, the County can increase utilization ratios and have greater data tiering flexibility to right-size storage and performance to meet application-specific requirements. With HPE virtualized SDN switches, network provisioning is streamlined, making it easier for us to monitor connections. For example, adding servers to VLANs is quick and easy because no additional physical cabling or networking devices are required.

Diverse applications share virtualized resource pools, so the operating environment automates HA policies to meet key performance indicators. A resilient, converged infrastructure provides the right level of availability for each business application.

Process to Measure and Correct Capacity: Capacity planning services for the County's workloads will be an expansion of services provided today. Figure 121 outlines HPES' ongoing capacity management approach that has proven effective within the County environments.

Figure 121. HPES Capacity Management



Through our experience with capacity planning, we understand the importance of being aware of external requirements, such as State or Federal mandates, that can affect the underlying technology demands. HPES will continue to collaborate with the County to establish thresholds and project application workloads. We combine this information with infrastructure utilization data to create tactical and strategic capacity plans to verify that the County's environment in Tulsa will accommodate growing and changing business requirements without jeopardizing performance standards.

We designed the MPC infrastructure for the County to provide the capability to expand capacity quickly due to unforeseen circumstances or emergency situations. This infrastructure is supported by HPES data center professionals who understand the County's business and technical needs. We use our industry-standard software tools to monitor and measure storage capacities and server central processing unit (CPU), memory, disk, and input/output (I/O) utilization and performance on a daily basis.

We analyze daily and monthly capacity reporting to identify and address day-to-day capacity constraints. Additionally, we analyze capacity trending reports to identify recurring problems that require system upgrades or system refreshes. We will continue to assess the impact of all changes on the capacity plan and the performance and capacity of all services and resources; tune and optimize the performance; implement County-defined policies; and develop methods to effectively monitor, measure, and report on capacity across the environment. We will also work with the County business owners as they capture forecast demand to produce and maintain a quarterly Capacity Plan that defines planned server system upgrades and refreshes based on growth of existing as well as new application workload. The team will update the existing capacity plan to reflect each year's forecast. Capacity planning for the County encompasses the following:

- **Servers** – Capacity management services for servers and mainframes and associated storage include monitoring system usage and capacity by analyzing historical resource trends. We continue to apply this data during decision-making reviews to assist in formulating environment requirements that meet or exceed future business requirements. Such capacity planning can enable greater efficiency and reduce required resources. Our comprehensive suite of server management and monitoring tools will monitor the servers against thresholds and alert operations when there is an issue. Metrics are captured and run through a data warehouse for trend analysis and capacity planning. Monitoring metrics are summarized each day and reported.
- **Planning for Increased Application Usage** – We enable performance analysis and availability management to allocate capacity dynamically based on HPES' in-depth knowledge and experience in resource allocation in a variety of County processing environments. We will continue to use system metrics and statistical reports to gain a clear understanding of overall capacity trends and performance. HPES and the County can use this information during decision-making reviews to reshape the compute environment periodically.

- **Network Capacity Planning** – HPES and AT&T will continue to monitor data network usage and performance and generate capacity reports that identify actual and potential network bottlenecks, by establishing capacity benchmarks and by analyzing trends. Such trends address the form of overall throughput, percent usage, error rates, and specific performance metrics such as packets per second. Our metrics measure both peak and average performance. We will offer network capacity recommendations for tuning the network to improve efficiency and cost effectiveness.
- **Storage Capacity Planning** – HPES designed the storage infrastructure for the County to support the ability to expand capacity quickly due to unforeseen circumstances or emergency situations. We use our industry-standard software tools to monitor and measure storage capacities, disk, and I/O utilization and performance on a daily basis.

2.9.4. Describe your proposed approach to hyper-converged infrastructure in the delivery of virtual infrastructure.

Hyperconverged infrastructure is designed to simplify design and management of the computing environment by merging and packaging the server, network, and storage components of infrastructure as well as management software into pre-sized building blocks. To achieve the simplification objective, hyperconverged systems would have to comprise nearly all of the infrastructure deployed in the data center; otherwise, a hyperconverged solution becomes just another platform that has to be integrated and adapted to the County's existing standards, which increases, rather than decreases, overall complexity in the environment.

As described in Section 2.9, Application Infrastructure Services (Schedule 4.3, Section 6.7), HPES will provide Helion MPC and Helion Managed Cloud Broker (HMCB) to be implemented during the transition period as we build the County's on-demand dev/test and production environment as part of the data center consolidation. These platforms help the County move toward greater standardization in the virtual/converged infrastructure environment. By implementing a private cloud with standard-sized building blocks of virtual infrastructure, we will be able to analyze whether hyperconverged infrastructure will ultimately yield benefits for the County. If we are able to fully standardize over time on the x86 platform in the converged infrastructure, then the next logical step would be to move to hyperconverged infrastructure as the data center components come up for refresh. When the County is ready for hyperconvergence, HPES stands ready to be the County's technology partner to accomplish this objective.

2.9.5. Describe your proposed approach to hybrid cloud integration with data center.

HPES' in-depth knowledge of the County environment and business objectives enables us to design a hybrid infrastructure strategy that most effectively applies to the County's portfolio of services, accommodates the required workloads, and enables desired business outcomes. Our hybrid approach to enterprise computing combines traditional IT resources for some applications—such as Solaris, HP-UX, AIX, and others—while Windows and Linux applications can be deployed in the cloud, as illustrated in Figure 1 in Section 2.9. The HPES hybrid solution for the County incorporates MPC services with traditionally hosted applications in the Tulsa data center, as described in Section 2.9, Application Infrastructure Services (Schedule 4.3, Section 6.7).

The HMCB layer enables the County to see all resources—traditional, private cloud, and, in the future (if desired), public cloud such as Amazon Web Services (AWS) and Microsoft Azure—as a unified infrastructure. Public clouds are sometimes suitable for applications that do not require storing sensitive data or specific physical machine characteristics. This approach enables the County to maintain centralized IT governance while effectively outsourcing and procuring IT resources from HPES as well as other cloud service providers. With HPES delivering and/or managing IT resources from the cloud, the County will see reduced costs and overhead, and gain the effectiveness and flexibility offered by cloud

services. Our design and architecture provide interoperability and integration of tools and common resources (such as storage, network, and security components) with the applications that remain in a traditional hosting environment, enabling smooth transition to hybrid IT.

Within our hybrid model, we built the MPC, customized to the County's requirements, that is scalable and works with the County's infrastructure. We have optimized the County's applications, as described in the Methodologies and Key Processes section of Application Infrastructure Services (Schedule 4.3, Section 6.7) to identify which applications should be in the MPC and which we recommend remain as traditionally hosted. As noted in Section 2.9.4 above, at such time when the County is more fully standardized, a move to hyperconverged infrastructure may be an appropriate next step. As a core HPES strength, we will work collaboratively with the County to continually assess the environment to make certain we maintain the optimal mix of hybrid infrastructure. Defining the right mix helps to increase efficiency and reduce cost.

We recognize this is not a one-size-fits-all or an all-or-nothing approach; our modular approach meets the County's needs for a mixed infrastructure that will evolve and shift over time. Our approach takes into consideration the County's evolving business needs, security, cost, efficiency, availability, performance, automation and orchestration, and timing. Additionally, upon integrating hybrid cloud, we consider open standards that avoid vendor lock-in as well as architectures with the flexibility to meet the County's changing needs. HPES recognizes the integration challenges; through our experience supporting the County, we are prepared to address these as follows:

- Continue to support and integrate with the workloads that currently run the business
- Integration must bridge the current applications and workloads with those planned for the future
- Applications differ in how they are designed, hosted, and consumed
- Applications have different infrastructure requirements

HPES uses a single management toolset, described in Section 2.9, Application Infrastructure Services (Schedule 4.3, Section 6.7), to manage different types of resources. Policy-based placement makes certain we deploy workloads to the right infrastructure based on specific business requirements.

2.9.6. Describe, in detail, your provisioning process for physical and virtual servers.

As described throughout the proposal, our hybrid solution for the County includes Helion MPC services combined with traditional hosted services. In the following paragraphs we describe the provisioning process for both of these environments.

MPC Provisioning: Implementation of HPE's Helion MPC enables us to quickly deploy new services where virtual infrastructure is automatically provisioned in hours or less instead of days, upon approval from the County. To provision virtual servers, upon approval by the County we will finalize the approved Solution Design Document (SDD) or Confirmation of Server Requirements and perform the following tasks for MPC server provisioning:

- **Access the MPC Provisioning Tool** – This provides an intuitive graphical user interface that HPES will use to select from a prepopulated catalog of services that we will define during the MPC build, including provisioning of virtual servers.
- **Browse the Service Catalog** – Using the catalog, we browse all predefined offerings and select the primary service desired to initiate the provisioning process.
- **Configure the Requested Service(s)** – Once we have selected a primary service to reflect approved County requirements, the associated selectable options will be available to our MPC provisioning team. For provisioning virtual servers, we choose the County's required minimum SL, the server name and size including quantity of CPU, RAM, and primary disk size, network connections, server OS, and target resource pool (applications infrastructure, infrastructure, or dev/test). We then select from a list

of predefined templates, which are the County's gold images. Next we can choose to add-on optional services such as predefined backup and storage choices as required to meet the County's specific workload requirements. We then add the item to the cart and repeat this process as needed to configure multiple approved servers simultaneously prior to checkout. Note: We can also reorder or place a request to initiate new services based on prior requests; this streamlines the process.

- **Place the Order** – When the configuration is complete, we review and confirm the requested items and confirm the new service(s) or modifications to existing services.
- **Order Fulfillment** – The HPES initiator receives notification when the automated order fulfillment process is launched, and continues to receive status notifications until provisioning is complete. We will notify the County once the services or changes are ready.
- **Manage Service Orders** – Notifications enable us to track order status in real time. We can also access, monitor, and perform actions on services (such as modifications, cancellations, or deletions), view a detailed list of all orders, and approve requests. Once a service is marked for deletion, a 7-day retention policy is enacted to safeguard the data in case this process needs to be reversed if requested by the County. Additionally, we can track status of servers such as Online, Offline, Transitioning, Reserved, Deploying, Modifying, Modification Failed, Failed, Canceling, Cancellation Failed, Expiring, and Expiration Failed.
- **Manage Services** – For services currently subscribed and running, we can view detailed information about the services and topology as well as the individual components that constitute the overall service delivery. Within this view, we can also request actions such as start, stop, reboot, create or revert snapshot, server resize, and more to manage the County workloads in an expedited manner.

MPC provisioning is powered by the following underlying technology and processes:

- **Cloud Service Automation (CSA)** – Combined with Operations Orchestration (OO) and Matrix Operating Environment, CSA automatically enables the design and provisioning of virtual infrastructure services in hours instead of days. HPE Server Automation software enables us to automatically perform activities such as server discovery, provisioning, patching, configuration management, and script execution to comply with IT configuration standards.
- **Computing Services** – HPES preconfigures the image for automated provisioning. Using administrator privileges, we provide OS patching and ongoing maintenance as well as all database and application installations, patching, and ongoing maintenance. We monitor system availability and security, and perform root-cause analysis and corrective action of OS; physical and virtual servers; storage, backup and network environment problems; and all other IT Service Management functions.
- **Storage Services** – HPES Helion Storage Services enable efficient information management while maintaining the right level of storage from creation to deletion. We will manage the County's active system data via a storage area network (SAN) platform using tiering technologies to balance cost and performance; this delivers a lower-cost solution, increases business agility, and minimizes risk. We also virtualize storage resources to increase utilization and provide greater data tiering flexibility.

  We provision storage infrastructure (hardware, software, and management tools) to store application and database data from the corresponding computing environment. Features include storage performance and capacity planning, monitoring, reporting, asset management, service operations management, and supplier engagement, when necessary. Details on the storage architecture for the County are included in Section 2.9, Storage Services (Schedule 4.3, Section 6.12).

- **Server Provisioning, Monitoring, and Management** – We install this service and configure it to meet County-specific needs based on the following:
  - Resource pool location for capacity provisioning
  - Availability "System Level" end-to-end Service Level for availability
  - Server size (CPU configuration: x-small, small, medium, large, x-large)
  - Server size (GB of RAM: x-small, small, medium, large, x-large)

- **OS Provisioning, Monitoring, and Management** – We install a standard build for the Windows and Linux operating systems and monitor availability of the servers and the OS instances up to the point of connection with network demarcation. Upon detection of an availability, capacity, or performance event, we investigate the outage and perform corrective action to restore the system. We also deploy local admin users for HPES Private Cloud Operations OS administration. HPES' OS management includes startup and shutdown, OS patch management, and maintenance job scheduling (at the OS and system level) for private cloud internal management activities.
- **Policy-driven Automated System Provisioning** – We automatically provision new cloud infrastructure based on defined policies. New systems are deployed once approved by the County, and we will periodically advise the County when new OS versions and editions become available.

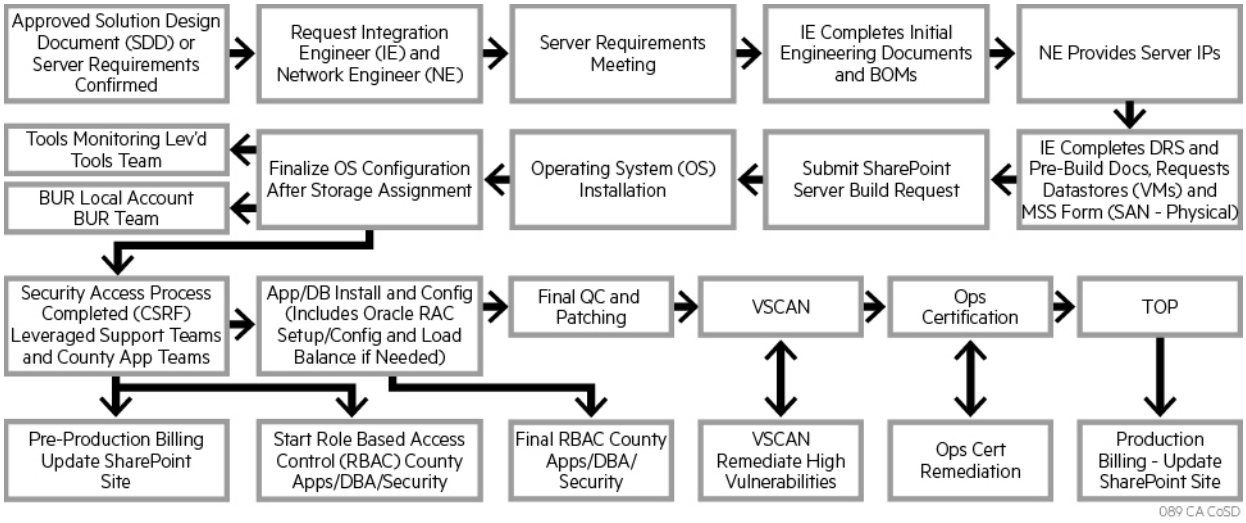
Traditional Provisioning: Using HMCB, we can perform automated provisioning of VMware servers in the traditional environment. Over the long term, we recommend that all VMware environments within the data center be moved into the MPC and the HMCB provisioning process be used for non-data center servers. The provisioning process for VMware servers in the traditional environment follows the steps above up to the point of layered product installation, at which point we follow the traditional process, described below.

HPES has an established and thoroughly documented process to provision traditional servers that begins when the HPES server team receives an approved Solution Design Document (SDD) or Confirmation of Server Requirements from the County, illustrated in Figure 122.

This process incorporates all the necessary engineering activities and includes installing the OS, configuring the necessary storage capacity, applying security controls, scanning for vulnerabilities, testing, deployment into the production environment and finally providing appropriate access to the Applications team to start development or testing as needed.

Adherence to this process will enable HPES to meet the County's Provisioning Service Levels.

Figure 122. HPES Standard (Traditional) Server Provisioning Process



Physical Server Provisioning follows the same process as Traditional Server Provisioning, with the following steps added, following the approval of the SDD:
Workload Placement is a step that engages the Hardware Planning team to determine the floor and rack locations and provide any additional power and cabling, if required.
Network Configuration: Switches and remote access capability are configured.

Hardware Installation: If sufficient hardware is available within the pool of spares, this hardware will be integrated and installed and connected, once the floor and rack locations are ready.
Procurement will occur to replenish any spares used by the request; or, for large or specialty hardware orders, this step will occur before hardware installation.
Storage Configuration: SAN fiber is connected and LUN allocations are presented to the physical server.

2.9.7. Describe your proposed management and support approach for the development and test environment.

We describe our approach to managing and supporting the development and test environment in Section 2.9 (Schedule 4.3, Section 6.9) of this proposal.

2.9.8. Describe your proposed approach to migrate E-Mail Services to the cloud.

We describe our approach to migrate email services to the cloud in Section 2.9 (Schedule 4.3, Section 6.10) of this proposal and in Section 2.11 Transition Services – Transition Projects: Email Services (Schedule 2.1, Section 3.2).

2.9.9. Describe your proposed process to classify County data to match required storage tiers.

As the County relies more heavily on electronic transactions to streamline services to citizens, data volumes will grow continuously as more business is transacted electronically by completing end-to-end processes on line. Currently, the County generates and currently manages nearly 1,200 TB of data; as this grows, storage costs grow as well. Managing data growth requires definition of data management policies for data movement and managing data storage to target cheaper storage based on data classification and the need to access, archive, and re-access data. Classification can imply the County's standard sensitivity classification structure: Public, Sensitive, and Confidential; however, classification can also be extended to permit very granular categorization to support specific policies.

Currently, documents are tagged as they are ingested. These tags can be used by the County's existing document/records management system to direct unstructured data to different tiers of storage. To address this challenge, HPES will use a technology-oriented approach to analyze and auto-classify the data (please refer to Section 2.12, Transformation Services). Over time, classification and metadata tagging can be done in a more automated way, reducing the need for manual tagging during ingest. Technology has matured greatly, and there are multiple products available today that provide the capability to identify, analyze, and control content across multiple repositories and apply policies to data to make sure it is managed optimally—for both functionality and cost—now and into the future, as the County learned from a recent assessment of this technology. In addition, HPES has a tool suite, ControlPoint, which we fully describe in Section 2.12 Transformation, of this proposal that helps us to classify data and assign it to the proper storage tier. ControlPoint uses the HPE IDOL (Intelligent Data Operating Layer) Connector framework to identify, analyze, and control diverse types of information stored in enterprise repositories. ControlPoint helps us to categorize information and apply policy to content indexed by IDOL. A dashboard-style display provides valuable business insight into the themes, locations, and value of County information.

HPES' in-depth knowledge of the County's existing data environment and first-hand experience with data management tools and storage enable us to help the County accurately classify data as Public, Sensitive, or Confidential and store data appropriately. Our structured four-step process for data classification includes the following:

- **Understanding the Landscape** – The process begins by gaining insight and understanding of the legacy and "dark data" landscapes. We define dark data as information assets collected as normal

business activity, but these are generally not used for other purposes. We then create a Solution Roadmap illustrating the go-forward plan and Return on Investment (ROI) for the organization. For the County, we will accomplish this by sampling approximately 1 TB of data currently residing on the County's existing file share environments. The assessment will showcase where unstructured data exists and how frequently is it being referenced/used so that intelligent decisions can be made around data management, archiving, retention, and retirement.

- **Develop data categories** – Using automated tools and common categories, we develop a set of categories specific to the County such as Public, Sensitive, and Confidential. We select a set of representative documents from the County's data repositories to use for training and benchmarking. This makes certain that the categories created are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content. Preparation of these draft categories will not affect documents in production systems.
- **Refine and Test** – To determine the relevance of the categories to enterprise documents, refining a category is done by adjusting the weighting of a term, the selection threshold, or by adding a field text. These activities can be done individually or in combination. A category can be published, making it available for use in automated policy execution against content managed by the tool suite.
- **Auto-Classification (requires Transformation project – see Section 2.12)** – Once unstructured data is categorized, we apply policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents. Using the desired tool suite, we can automate policy application and govern all aspects of the information lifecycle including deletion prevention, storage management, and ultimately disposition management by applying policies at data creation. Additionally, de-duplicating unstructured data across repositories helps to minimize storage costs and reduce discovery times.

2.9.10. Describe your proposed approach to further integrate data with Backup and Recovery Services, using required connectors such as Oracle RMAN and VSS.

HPES' Oracle Administration uses RMAN to write database backup files to spinning storage that is made available on the database server for this purpose. This approach is more efficient and less disruptive than writing RMAN files directly to the backup system. The backup files on spinning disk are then captured in the next HPES Data Protector backup. The files will be stored on our tapeless backup media and replicated over a dedicated replication network connection to the DR site hundreds of miles away in Colorado Springs, meeting the offsite backup media storage requirements. We support the creation of VSS (shadow copies), and the HPES backup solution can also back up VSS shadow copies directly with a local copy of that backup written to the tapeless backup target and replicated to our remote backup media, as previously described. Currently, HPES successfully follows this methodology to back up all of the County's Oracle databases.

Data Center Services Framework – Executive Summary

HPE Named a Leader, Gartner Magic Quadrant for Data Center Outsourcing and Infrastructure Utility Services, North America

In this report, published in July 2015, clients rated HPES as follows:

- HPES earned high marks for uninterrupted quality service,

As we designed this solution for the data center services framework, we made all of our decisions with an eye to the end result: a reliable, predictable, secure, and more efficient IT infrastructure to deliver superior public value to the County's constituents through continual improvement and innovation. We looked at not only the components of the data center services framework and how these must seamlessly integrate within the framework, but also how data center services integrate across the frameworks. Our solution provides the following differentiators and benefits:

effective end-to-end management and budget oversight.
- HPES has many ITIL-certified personnel and processes, which helps it to consistently deliver services and consistently overachieve on SLAs.
- Many clients state that HPES understands their business requirements and is agile and equipped to manage the requirements effectively.

- A hybrid design that is common for all three types of servers, yielding greater levels of reuse, consistency, quality, and efficiency than would be possible with three separate solutions.
- Cloud Broker automation that extends the County's hybrid IT reach into the public cloud when needed, without additional data center infrastructure.
- A solution that balances the need to maximize current investments and application stability during transition, while positioning the County to achieve its objectives for greater standardization and virtualization.
- A low-risk transition: more than 50% of the current infrastructure and 100% of the support staff are already in their post-transition location.

Our Data Center Services solution integrates with other frameworks as follows. Note that workflow automation applies to services provisioned under either MPC or HMCB; services in the traditional hosting environment are provisioned using task-level automation.

- Provides workflow automation for deployment of cross-functional tools for capacity, performance, security, and asset and configuration management
- Provides workflow automation for provisioning of data center network resources
- Provides faster time to value for the Applications Services Framework by creating environments on demand
- Provides more efficient utilization of resources for the Applications Services Framework by effectively implementing dynamic environments
- Supports efficient Disaster Recovery Services by leveraging the replication architecture to support both DR and offsite vaulting requirements
- Integrates with the Service Portal: all deliverables and outputs will be posted to the Service Portal as required; however, in the future, the private cloud and HMCB interfaces themselves can be integrated into the Service Portal if and when the County is ready to move to a self-service implementation

Competitive Differentiators: Below we list several unique key points and themes related to what HPES can offer the County; these are reflected throughout our response. These attributes, and their benefits to the County, include the following:

- **Understanding County Business:** Through our experience working side by side with the County, we strive to understand priorities, goals, objectives, preferences, and approaches. This is applicable to governance, reporting, County interactions, and delivery of services. We educate every new employee supporting the account on County business and make certain they know how to deliver services to meet or exceed County expectations. HPES welcomes the opportunity to continue the IT journey with the County.
- **Reliability:** The County has a critical mission in providing services to residents, including support of initiatives like Safe Communities, Sustainable Environments, and Healthy Families. Many of these services rely on the IT systems HPES supports. We have consistently met service levels and received

high marks on outage management. Our staffing, processes, procedures, tools, and experience enable us to work with the County to provide this high level of service. County residents and County employees have received great benefit from this reliability.

- **Predictability:** We recognize the importance of predictability in the annual budgeting process. We understand this process well, and we understand that the County will rely on the cost inputs we provide. We are diligent in our estimating so that our costs are reliable and predictable and help the County to avoid budget issues.
- **Innovation/Technology Leadership:** HPES is a recognized leader in the IT industry and has been at the forefront of technology innovation. We recognize that local government depends on getting the right technologies in place to support the new era of digital government services; we can provide those technologies. HPE Labs invests more than $2 billion per year in research and development to bring innovation to our clients. This includes investment to develop one of the broadest portfolios of cloud services in the market. At the local (account) level, we created an Innovation Council to identify and develop new ideas, technologies, and processes to benefit the County. The council's intent has been to address real business needs and reduce cost as well as to increase efficiency and productivity. The next step in the evolution of the Innovation Council will be to add representation from HPE Labs and forge a sustained relationship between the County Technology Office (CTO), the HPES account, and HPE Labs.
- **Personnel/Staffing:** Our team—whose experienced, highly qualified members are primarily San Diego County residents—has consistently demonstrated their commitment to deliver high-quality services to the County. In addition, this team is knowledgeable of County business and demonstrates that knowledge in every aspect of contract performance.
- **Depth and Breadth:** HPES, as a world-class provider of IT services, has the capabilities necessary to support all the requirements of this large, complex contract. Along with our key telecom partner AT&T, HPES has proven that we have the depth, breadth, and staff to deliver the full scope of services. In addition, HPES is a stable, recognizable, financially strong company that the County can rely on to be your trusted partner and provider for the long haul.

With a well-planned approach and continued support from HPES, the County will have the tools it needs to effectively carry out its strategic initiatives for Safe Communities, Sustainable Environments, and Healthy Families. Protecting the County's data and systems is vital to HPES. Our approach delivers the data center framework components built on a reliable, integrated information services environment to help the County achieve its mission to efficiently provide public services that build strong and sustainable communities.

2.10 Applications Services Framework

Executive Overview

The County recognizes that a well-functioning, streamlined portfolio of applications is the foundation for providing efficient services to employees and residents. In recent years, the County has rationalized their portfolio of applications from 540 to approximately 400. This eliminates the costs associated with extraneous applications and combines similar functions for multiple departments into standardized enterprise applications such as SharePoint and CRM. HPES has been your trusted partner in rationalization and other endeavors—responsive web applications, PeopleSoft upgrades, and the award-winning JELS and PUMA apps to name a few. We understand the current County environment and look forward to partnering with you to leverage new technology and best practices for continual business efficiency and transformation.

The HPES approach is to provide high-quality, cross-trained applications services support staff who know the County's way of doing business and are deeply familiar with your applications. The core of this group will be the staff who provide services today with additional SMEs for specific business technology requirements (CRM, mobile development, among others).

- Applications Maintenance & Operations (M&O) Services - The County's objective is to improve cost predictability and incentivize proactive steps by the Provider to increase efficiencies and maintainability of production portfolio applications.

HPES is proposing a bundled approach. Applications will be bundled based on level of service appropriate to each bundle by Business Group. On a quarterly basis, or as requested by the County, we will review the application portfolio with the County to determine growth or reduction of applications and determine if a bundle adjustment is required. As a part of the review, HPES suggests establishment of an Application Review Board (ARB) to evaluate the activity and provide "move forward" recommendations.

The Application Review Board, with participants determined by County CIO and Contractor AE, shall review all impacted billing low-orgs to determine if growth or reduction adjustments are required to either one or more Applications FFP bundles or the FFP Dev/Test RU. Annual pricing reductions to the FFP M&O will be 2% beginning contract year 2.

The applications are separated by bundles types into three groups—(full support, coordinated support, and Software as a Service (SaaS) support) across the five business areas, as identified in Exhibit 16.1-5 of the RFP.

	Concept Considerations	**Concept Considerations**
By County	3 RUs (one for each bundle type)	Allocation to be determined/executed by County
By Business Group	15 RUs	Further allocation would be determined/executed by the County.
By Low Org	131 RUs	Assumes 47 depts., some may not have all 3 RUs. Low-org may be a better grouping as HHSA often uses a single low-org regardless of Dept.

The larger the group the more tolerance for change. For departments with only 1 or 2 applications, if they remove applications the impact is greater than those with 20 applications.

Our M&O solution provides the County with the cost predictability departments require to forecast accurately.

- Applications Development Services - The County's objective is to provide greater reach and access to Applications providers, products, and services for County departments seeking to improve business operations.

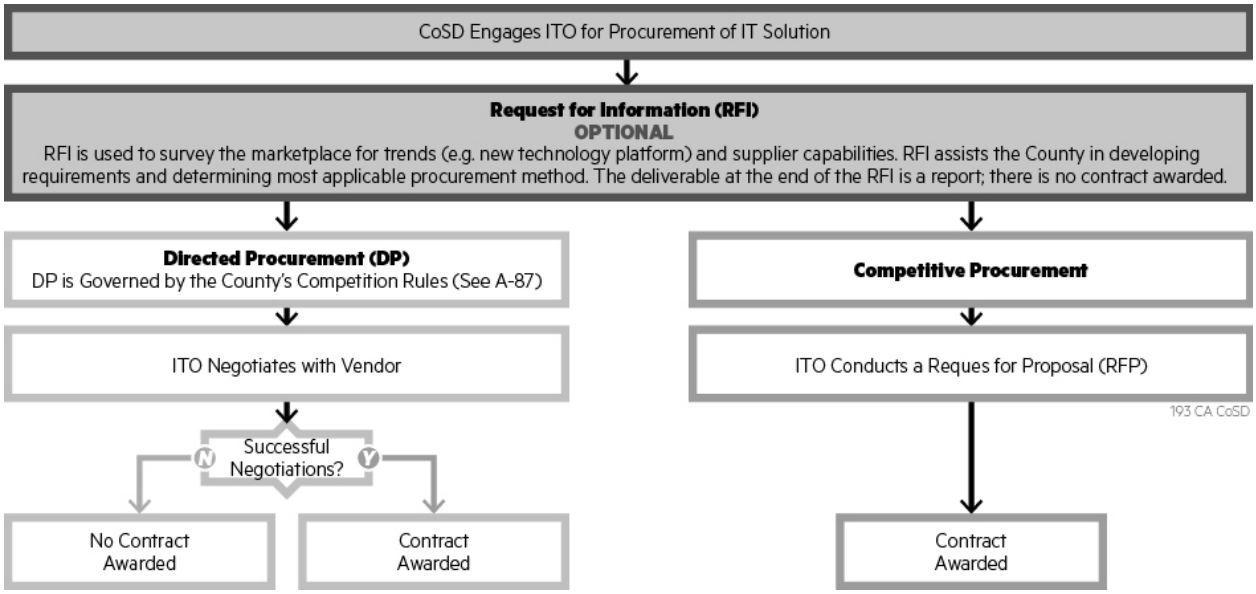
HPES will reach out to application providers who can deliver quality apps projects on time and within County budget. As builder for some, broker for all, we do not assume HPES must develop all County projects with HPES personnel. We will work to include applications providers such as SAIC and CGI in our outreach process that currently includes more than 20 providers, such as The Select Group, TEKsystems, Lockheed, Nicus, Apex Systems, and Insight Global. We will also reach out to Disabled Veteran Business Enterprises (DVBE) and give them the opportunity to provide services.

HPES will continue to work with the County to use COTS and third-party applications where appropriate. On a per project basis, we will reach out to third-party providers as resources and expertise is needed. If the County has a requirement for a specific or unique solution, we will engage with those application providers as described in the "Procurement of Third-Party IT Solution via the ITO" process referenced below. Note: This document is under development/review with CTO.

Currently, third-party vendors have access to the development and test environments and this practice will continue.

Figure 123 outlines the proposed Third-Party Procurement process designed by the County and HPES. This process outlines how the County can utilize HPES and the ITO contract for procurement or inclusion of third-parties in solutions.

Figure 123. Third Party Procurement via ITO



Application Maintenance and Operations Services (Sched. 4.3, Section 7.2)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

HPES has provided IT operations and management for more than 40 years, and has supported the County using approved procedures and our operational excellence methodologies for the past 10 years. Our

application M&O solution will build on this foundation while identifying opportunities to improve M&O support and the overall IT environment.

Our solution will include the transition of all of the County's M&O activities to the FFP model. In our discussion below of 10 high-level M&O requirements that follow, we will distinguish between M&O activities and development activities.

We have selected Tina Terlecki as the Application M&O Manager. The County knows Tina as a collaborator and leader in implementing innovative IT initiatives. An integral part of our leadership team, Tina will use her 16 years of experience supporting the County and her deep familiarity with its applications and IT infrastructure to drive continuous improvement in this area.

Restore service levels

First, we will validate the restoration requirements for each application and structure our team to meet those requirements. If an application requires 24x7 onsite support for restoration of services, we will staff and schedule the response team to be sure M&O staff is available 24x7, as we do today. If an application requires 24x7 on-call support, we will schedule staff to be standing by to respond to an outage 24x7. Applications that require less than 24x7 will be supported in accordance with priority to specific County business needs. HPES currently provides a Monday through Friday, 6:00 a.m. – 6:00 p.m. support window for all other applications; we will continue to provide this window.

HPES will build and enhance applications to prevent outages. As part of application portfolio maintenance, we will design and develop applications to be hardened and not fail. We will evaluate the supporting software middleware and hardware for the application to verify the application's supporting components deliver required performance without disruption. Our team will thoroughly test the application's new functionality, regression test unchanged functionality, and performance test the application executing simulations in a Test/Dev environment before implementing a change. The HPES application build process is based on our experience and best practices, including ITIL-aligned processes and CMMI standards.

HPES will operate to restore applications functions as quickly as possible in the case of outage, whether application or infrastructure based. HPES will follow the Incident Management process detailed in Section 2.5, Cross Functional Services. Technical support will triage as soon as they are notified by the Service Desk, and continue to work the issue until functionality is restored. For mission-critical outages, the support staff will use additional SMEs as needed and reach back to vendors and suppliers when necessary to resolve the outage. The Service Desk, with information from the technical support staff, will notify HPES management of the outage, and HPES management will notify County management. The escalation process is detailed in Section 2.6.

When a change to the application is required to resolve the outage, HPES will perform the necessary application changes, data updates, and/or third-party software patching, to restore services in accordance with County emergency fix process. All application patches for routine maintenance and/or restoration of services will include user acceptance testing as desired by the County.

No plan to restore services would be complete without mentioning the effort to prevent defects in the first place. Our application services team will build new applications and enhance existing ones to prevent outages. We will make recommendations for changes to applications, and perform analysis to identify defect rates, annual cost, and technical obsolescence within applications. As part of the ARB, HPES staff will work closely with the County board representatives and present outage incidents, provide recommendations regarding obsolete processes, and review portfolio additions and deletions. A standard agenda will be developed and reviewed at each meeting.

Production portfolio applications maintenance

Our plan to maintain the portfolio focuses on keeping production up and running with a goal of no disruption to the County. In addition, we must continually improve many applications to optimize performance and apply patches from third-parties. The key to minimizing impacts to production is to thoroughly vet any change prior to promotion to production.

HPES will make maintenance changes to production applications upon a County-approved request for change (RFC). We will meet weekly with the County to review the pool of RFCs and determine the priority and whether it should be approved for implementation. HPES will schedule the implementation of approved RFCs based on County priorities.

When HPES implements an RFC to fix a bug, install a patch, or implement a simple upgrade as part of M&O, we will follow our existing SDLC methodologies and the County's change and release management processes, including receipt of required procedures in the governance process. We will functionally test RFC implementations and perform regression and performance tests. While implementing the change, we will build in warnings, notifications, and processes to provide application support of the RFC during operations if needed.

In conjunction with the County, we will define the authorization requirements (security) for end users, roles, and schemas and will provide provisioning and deprovisioning of user and service accounts for the portfolio applications as authorized.

If a firewall change is required by M&O activity, it is covered under Apps M&O. If the firewall change is required by a new application or new user request (adding DA or hospital access), it will be costed as part of the project.

With every service restoration fix, patch, or minor maintenance implementation, we will update the operations support manual in accordance with the new functionality in production and all application document artifacts impacted by the RFC, including application document libraries, configuration management databases, and application management system, known as AppsManager.

We will evaluate the applications architecture, configuration, and system upgrades and identify opportunities for improvement. When opportunities are identified, our team will initiate new RFCs and implement them after approval by the County.

In addition to implementing changes, our team will support the application in production. We will build an application support team with the right number of staff with the right skills set and expertise to support the applications in production. RFCs are implemented in adherence to our SDLC process, the County's change management and release management procedures, and County governance approvals. We will provide services based on ITIL-aligned processes, CMMI standards, and other leading practices as appropriate. HPES is committed to providing superior service in the delivery of the right solution for the County portfolio applications. Our experienced project managers and applications subject matter experts (SMEs) will continue to work with the County and its delivery and application product owners to build a project plan to provide predictable, repeatable, and successful results.

Our M&O services team will provide planning, monitoring, and schedules for new applications as they are placed into production. Should monitoring these items become permanent, we will update the Application Operations Manual. The team will respond to warnings and notifications generated by the applications and fix the issue that triggered the warning or notification. Our infrastructure support team will monitor the operating environment supporting the applications. HPES will triage application and hardware incidents and take the appropriate action to restore service.

HPES will execute user administration for the applications following the application's processes and procedures for user administration, including the necessary County approvals. We will update the Standards and Procedures Manual as necessary as well as Service Desk scripts, application data elements in AppsManager, and the new Service Portal described in Section 2.6.

Our periodic reviews may result in recommendations for application security improvements, product and software changes, or improved performance and cost savings. We will provide recommendations to County business owners and CTO to make sure the performance of the applications portfolio is optimal.

As part of M&O activities, our staff will perform special testing for events such as public holidays, end of financial year, end of calendar year, and daylight savings time.

M&O activities include executing the process to maintain application interfaces and coordinating with third parties to manage those interfaces. M&O includes performing the necessary routine system patching and application upgrades as well as code releases for restoration of services and maintenance release not resulting in enhancements or new functionality.

An enhancement is described as any product change or upgrade that increases software or capabilities beyond original specifications. It can also be distinguished as an improvement (enhancement) of an existing application capability from a totally new capability.

- Our fixed-price M&O RU includes preventive maintenance, application updates, and patches (that do not involve new functionality or features), and all activities required to achieve restoration of service/ break/fix.
- M&O includes performing the necessary routine system patching and application upgrades as well as code releases for restoration of services and maintenance release not resulting in enhancements or new functionality.
- Upgrades for the application that will provide new features and/or functionality will be supported under application development services. (For example. PeopleSoft 9.2 upgrade).

Figure 124. Application M&O Scope

Covered Under M&O	Not Covered Under M&O
• Updates that Maintain Current Features and Functionality • Restoration of Service • Preventative Maintenance • Application Updates and Patches	• Updates that Provide New Features and/or Functionality • Developments and Integration Activities

191 CA CoSD

In the event of a service outage resulting from application or infrastructure abnormalities, our M&O staff will perform necessary code fixes to restore service in accordance with the bundled service. The SDM will drive incident management activities and provide ongoing communication to the client. As a result of the service restoration, we will execute the necessary root cause analysis (RCA) to investigate the outage issue, following the RCA process as described in Section 2.5, Cross Functional Services. These activities include analysis, design, coding, testing, data conversion, documentation, user coordination and communication, and production turnover activities and the management of these activities for restoration of service. Based on the RCA findings, HPES will recommend modifications to the application to prevent future outages, including those attributable to a third party.

Align Maintenance Activities with County architecture standards, guiding principles, and architecture bricks and patterns

HPES' plan is to continue to align with County IT architecture standards while participating in the process to improve, refine and enhance them. As your current IT provider, we are in the unique position of leveraging our existing knowledge of County standards to continue to deliver the latest technologies.

We will monitor technology trends, best practices, and products within the IT industry, recommend enhancing County processes when appropriate, and provide a repository to document and manage standards. We will build any additions into standard processes and practices.

On an agreed to schedule, we will participate in annual technical and business planning sessions, including bricks, to enhance standards, architecture, and project initiatives.

HPES will perform maintenance activities following the Standards and Procedures Manual as updates occur and will implement all modifications to make sure our staff is aware and trained.

Provide M&O services for portfolio applications in production environments including servicing middleware and other application supporting components.

HPES will maintain both Dev/Test and production environments for applications. This maintenance includes keeping Dev/Test configurations synchronized with production. Our M&O staff will keep the application and its supporting components, such as middleware, synchronized. We accomplish this by updating supporting components using the same processes we use to update the applications. Our M&O staff will initiate an RFC to update components and implement the update when approved and scheduled by the County.

We will put steps in every project schedule to update the Dev/Test environments with any approved component upgrade.

Maintain accurate and continuous prompt updates to asset and system documentation

Every project plan will include a step to update application documentation. This includes updating asset and system documentation and tools. M&O staff will be responsible for the technical accuracy and specific details of the update, and staff leads will review the changes for accuracy and completeness.

Validate cross-framework integration and communication is conducted for application incidents, outages, maintenance work, planning purposes and all changes

HPES will validate cross-framework integration by regression testing application bug fixes and enhancements prior to production implementation. We will build and maintain test environments that include or simulate cross-framework integration, and we will build our test plans to include cases to test the frameworks

We will keep County framework leads and stakeholders informed on the full range of application activities from incidents, M&O activities, and changes. We will communicate at each step with County business owners and CTO.

For outages, the need for frequent, accurate information is paramount. The applications team will follow the outage management communication process described in Section 2.5.5.

Provide services in alignment with ITIL and CMMI standards to ensure predictable, repeatable, and successful results

We will use industry best practices to enhance effective planning, execution, tracking, and delivery of services to the County. HPES has a rich repository of proven methodologies and processes, enabling us to produce and deliver consistent service for the County. Our repository provides the backbone of our process improvements and includes templates, guidelines, checklists, and lessons learned. It complies with recognized industry standards, including the Project Management Institute's (PMI) Guide to the PMBOK, ITIL 2011, International Organization for Standardization (ISO) standards, and the practices incorporated in CMMI Institute's Capability Maturity Model Integration (CMMI).

By using these best practices and staying current with updates and changes, we will deliver predictable, repeatable, and successful services.

Implement new patches and versions (within the current release), prioritizing patches that address security vulnerabilities

We will implement new patches and versions under M&O following the existing RFC process. We will create a plan to communicate, test, and implement each patch or version. All patches and versions will be discussed with the County business owner and CTO to determine criticality, scope of change, priority, and timing. Following successful testing, we will submit an RFC for approval and scheduling.

When competing patches are released, patches that address security vulnerabilities will get priority, along with those that fix critical issues. Next priority would be patches that address minor issues, those which have a workaround available, and lastly patches that address issues that have not impacted County users.

Perform Maintenance Services that include Preventive, Adaptive, and Perfective Maintenance

HPES will perform application maintenance as part of M&O service. We understand the objectives of preventive, adaptive, and perfective maintenance with respect to M&O to be as follows:

- **Preventive Maintenance** – Maintain application reliability to prevent issues from emerging in the future
- **Adaptive Maintenance** – Modify the system to adapt to changes in the business environment.

- **Perfective Maintenance** – Modifications and updates to sustain application usability and improve its reliability and performance.

We will perform preventive maintenance to resolve known problems and defects; perfective maintenance to optimize and tune performance; and adaptive maintenance to remediate impacts resulting from interfacing application changes, changes to application middleware, or changes to the infrastructure.

Application Programming

Application programming are those activities associated with the programming, scripting, and configuring of application modules to support M&O activities.

HPES will perform applications programming using and adhering to the County's technical and architectural standards as well as standards and procedures, performing all necessary steps to complete M&O tasks. HPES is currently using Microsoft Team Foundation Server (TFS) and we will continue to use this tool to create working directories and store source code.

Application Integration and Testing

Application integration and testing are services confirm that individual application framework components work together properly and, as a whole, perform their specified functions.

HPES will plan and develop our testing procedures to meet County requirements and policies. We will document the testing procedures in the Standards and Procedures Manual, including procedures to be followed by an independent testing team as needed. HPES will develop an overall test plan for M&O releases that includes the test strategy, coverage, scenarios, test bed, test data, methods, schedule, and responsibilities.

To effectively test an application, HPES will build and maintain an application Dev/Test environment that has been refreshed with production data. If necessary, we will build data masking programs to disguise production data. HPES will build test cases to test the new functionality or components based on the requirements and determine which valid data is required to appropriately test the application as well as the various testing phases. HPES will create a set of test cases to test the application end-to-end, new and existing functionality, application security and application supporting components, and infrastructure, when needed, to support M&O activities. Benchmark test cases will also be created and run to properly execute regression testing. HPES will provide a reference to link requirements and test cases.

When testing an application, HPES will execute the test cases while following the standard testing procedures and verify that the results meet County testing requirements. HPES tracks defects in a County-approved tracking tool and corrects retests functionality to validate repairs. In addition to testing the application, HPES will provide an UAT environment, if needed, that includes the necessary data. HPES supports the County in its UAT testing effort and provides access to the defect tool for entering found defects. HPES will assess and report potential risks to production of implementing a change and only implement after County approval.

HPES will manage the various Dev/Test environments including the application data, application releases, and supporting software and components. HPES stages the applications changes in the appropriate system in preparation for production implementation. We will support these implementations, track their migration status, and verify the implementation of changes into production. HPES will define the test-to-production turnover requirements and instructions for each project or release and report the results, which will be shared with the County.

Application Implementation and Data Migration

Application integration and testing for M&O activities will be defined as those activities associated with the installation and migration of new patches and maintenance upgraded components to the production environment.

HPES plans to create a detailed plan for each M&O release. We will have a "go/no-go" checklists, after approval of UAT. All M&O releases will include rollback steps and, HPES will update any affected application documentation and production application support documents and procedures as needed.

HPES will execute, coordinate, and communicate with the County for all releases and associated activities. For each patch and/or upgrade, we will perform the needed steps of the SDLC such as requirements analysis, design, development, and testing as appropriate for M&O activities. Our deployments will follow the County's change and release management processes and are complaint with client change management policies. Documentation will be regularly updated, including the Standards and Procedures Manual and Service Desk scripts. HPES will execute the deployment in production once approved by the County and synchronize in-production environments by deploying the implementation in the application's Dev/Test environments.

Application Documentation

Application documentation is defined as the development and maintenance of documentation for all applications. HPES will continually improve application documentations, providing new and updated documentation when required for system specifications, technical documentation, operational processing flows, system installation, application production support manuals, configuration plans, tuning instructions, release notes, and solution design as needed for M&O upgrades and patches. HPES plans to execute application updates as needed with every release, including patch and update releases. New functionality will not be part of the update; rather it will be part of the application development T&M process.

HPES will build and maintain documentation folders for each application, which will be stored online with County controlled user access. All documentation created or updated for a release will be stored in the folder in DocVault and will be updated at the same time as the release implementation. This will help to keep the documentation in sync. HPES will store updated code and application components in the code CMDB to maintain the application currency and versioning.

HPES will also assist the County with developing, maintaining, and enhancing its application DR process and related documentation.

Application Training

Application training is defined as the implementation of training programs for contractor personnel to help preserve and enhance their knowledge and understanding of applications.

HPES will develop training for new and existing staff on the applications as necessary for M&O activities. When HPES builds a patch or service restoration release, we will update the application training plan as needed.

During application operations, HPES will provide technical training and knowledge transfer to existing County support personnel, as well as materials related to the technical aspects of applications, as necessary. HPES will develop, document, and maintain the Policies and Procedures Manual, training, and knowledge transfer procedures that meet the County's requirements and policies.

Application Quality Assurance (QA) Services

Application QA services is defined as a systematic, planned set of actions necessary for software update/development processes to conform to established functional technical requirements. It also includes the managerial requirements of keeping the schedule and resources within budgetary confines.

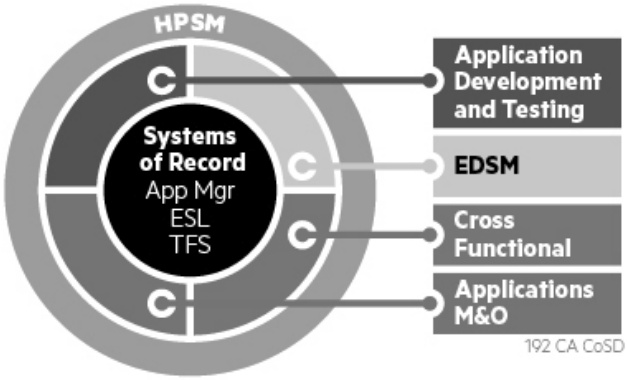
HPES will create, update, and maintain a QA management approach for applications updates. This approach includes the following QA components:

- Quality management approach
- Effective software engineering technology
- Formal technical reviews applied during the SDLC process
- Multi-tiered application integration and testing strategy and implementation
- Control of software documentation and associate changes
- Procedure to measure compliance with software development standards
- Measurement of QA metrics and reporting mechanisms.

HPES will submit our QA management approach to the County for approval, after which it will be added and kept current in the Standard and Procedures Manual.

HPES' determines QA metrics for each release and reports these to the County. We will communicate configuration management items, tracking them to our Systems of Record that accurately depicts the environment. These will be updated to reflect all new changes, which will be made with a change record processed through HPE Service Manager that keeps our information accurate.

Figure 125. System of Record



Database Administration (DBA)

Database administration (DBA) is defined as activities associated with the maintenance and support of databases.

HPES will define DBA requirements and policies for the application databases, including authorization requirements for End-Users, roles, and schemas. We will develop a Standards and Procedures Manual database administration procedure that meets the County's standards and policies. We will develop and provide database roadmaps for planning and portfolio management.

Our DBA processes will document security administration including managing role and end-user database permissions and in accordance with the County security policies. We will perform database restores when required.

HPES will define, document, and execute database creation, configuration, upgrades, patches, refreshes, database system-level changes, schema changes, and definition requirements for applications. We will maintain documentation for portfolio applications database instance parameters and system settings and manage them across like instances when required during the application change process. We will also execute proactive database performance and tuning scripts and monitor database performance for optimal performance.

HPES will implement and administrate County-approved appropriate database management tools across application portfolio database instances. We will capture performance metrics and historical data for trending and reporting. We are planning to utilize Oracle Enterprise Manager to manage the Oracle/UNIX

enterprise applications. In conjunction with Oracle Enterprise Manager, we will use the Applications Performance Management (APM) tool to provide a full 360 degree view.

Also, we will identify and resolve locking conflicts, latch contention, and rollback requirements for database instances and implement database monitoring tools that generate automatic Service Desk trouble tickets for incidents.

HPES will provide technical assistance and subject matter expertise to application developers and third-parties. We will provide data dictionary knowledge, end-user data assistance, data warehouse metadata definition, and data mapping assistance.

Our DBAs will patch database software as approved and manage database communication software configuration, installation, and maintenance. They also will provide database storage management and cleanup activities, backup schedules, retention periods and levels, and execute backups and recoveries that adhere to the County's policies.

Our DBAs will provide database capacity management and availability management, maintain database storage allocation, file systems current usage, and capacity. HPES will conduct database installation, de-installation and administration, testing, copying, and security and database server management, as needed and provide administrative account support that includes provisioning and deprovisioning. We will create and provide system monitoring and documentation, maintain transactional logs, and backup as scheduled. Finally, HPES will provide operational support for the County's public and private cloud databases.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

We will utilize our HPES Rancho Bernardo office, County locations as requested/required, and application development centers in El Paso, TX and Pontiac, MI.

- Methodology and Key Processes – Key methodologies and processes in proposed solution including year-to-year continual improvement.

We will use County-approved procedures and standardized industry processes and governance based on PMBOK, ITIL, and CMMI as well as the HPES operations excellence support methodology and repository of best practices and lessons learned. By driving the adoption of standards, taking full advantage of developments in technology, and being flexible and agile, HPES will help the County transform and manage its environment to achieve a balance of maintenance and innovation, reliability, and change. These methodologies will enable our team to prevent outages and defects before they occur by thorough testing during the development phase. Should an incident occur, however, our methodology provides responsive M&O for fast and effective resolution.

For continual improvement, we will regularly review incident reports, RCAs, and application performance data so that applications are optimized appropriately. We will also monitor industry best practices as well as emerging trends and new technologies to determine if a different solution would provide a better outcome. All this information will be shared and reviewed with the CTO.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES has automation tools such as our APM which provides a 360 degree view that verifies the performance of desktop, web, and mobile apps for on premise, cloud, or hybrid environments, as well as Cascade, SCCM, and various other network related tools

- The implementation of APM will enhance our ability to:
- Provide end-to-end visibility of transactions including back-end systems and mainframes
- Monitor the end-user application experience and services

- Quickly find and resolve application performance issues
- Collaborate with application development teams to effectively resolve application and transaction issues
- Reduce mean time to repair critical business transactions
- Monitor performance of applications deployed to a cloud or virtual environment
- View application performance alerts anytime, anywhere on your mobile device.

Currently, Cascade, SCCM, HPE Operations Manager, and other network and system related tools and reports are in place today and are being used to identify and correct issues in the environment related to applications, desktops, web, mobile applications, and others. The addition of APM will assist to close the circle of the end-to-end reporting so that HPES can be proactive in addressing systemic issues and making sure our solutions are running as expected to support the applications.

The SDMs will work with the application SMEs, vendors, and the Enterprise Problem Manager to make sure that any and all items identified through these tools and reports are being acted on quickly to reduce the amount of impact to the end users as described in Sections 2.5.5 Service Delivery Management and 2.5.9 Problem Management Services.

We currently and will continue to use the HPE Project and Portfolio Management (HPE PPM) module for consolidating, prioritizing, and fulfilling application services activities and development projects so the County has visibility into all of the demands on the infrastructure. Its web-based dashboards provide real-time visibility into request status, priority, next steps, and summary views. Service levels are updated automatically as each request is processed.

We will be rolling out a new Service Portal that will automate Service Desk ticketing, as described in Section 2.6, for incident and break/fix resolution.

On an ongoing basis, we will evaluate additional tools to further automate M&O activities, such as self-healing tools and discuss any recommendations with the County.

- Qualifications and Experience – Background and experience in comparable environments

HPES has more than 50 years providing applications M&O to thousands of clients and 10 years providing application M&O to the County. HPES monitors and supports approximately 400 steady-state business applications across all five of the County's business groups and provides expert troubleshooting, problem resolution, and infrastructure sustainability.

HPES manages all aspects of the California Department of Corrections and Rehabilitation (CDCR), which is responsible for Strategic Offender Management System (SOMS), an integrated electronic offender management information system. This is one of the largest IT deployments in corrections in the United States. We provide a full range of IT solutions and applications development services that include program and project management, testing, business intelligence and analytics, database support, imaging, and technical support. HPES hosts the SOMS system in our Sacramento data center, providing 24x7 production support for the system, its infrastructure, and interfaces.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

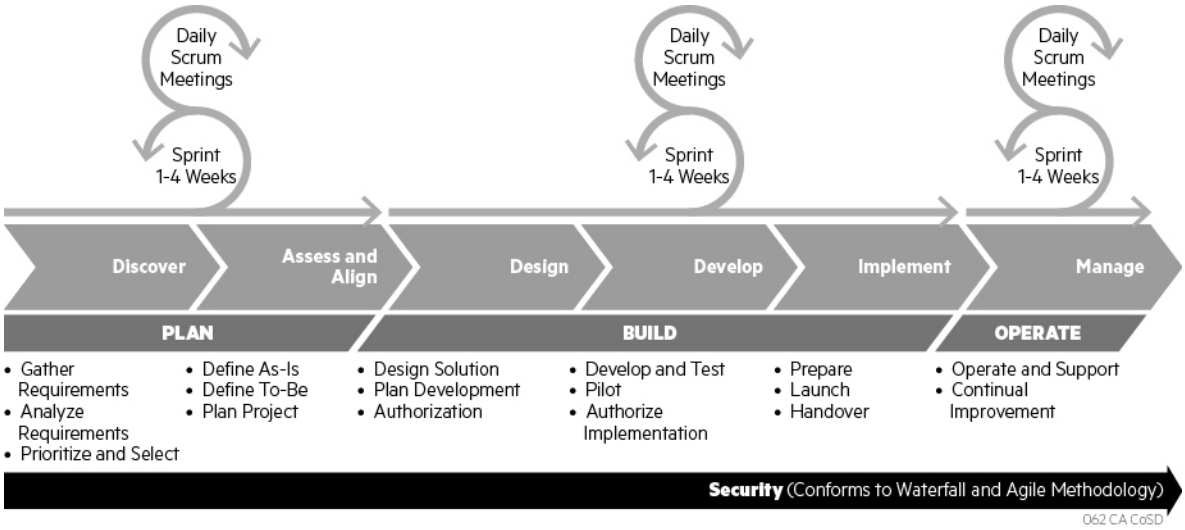
None.

Application Development Services (Sched. 4.3, Section 7.3)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

Our solution uses an established HPES application development framework — plan, build, operate — to meet deliverables requirements. This framework accommodates Agile, Iterative, and Waterfall methodologies, making sure roles and responsibilities are defined, governance processes are in place, and the work follows a structured approach to achieve its objectives. Our applications team will tailor the framework, as shown in Figure 126 to meet all County requirements.

Figure 126. Application Development Framework



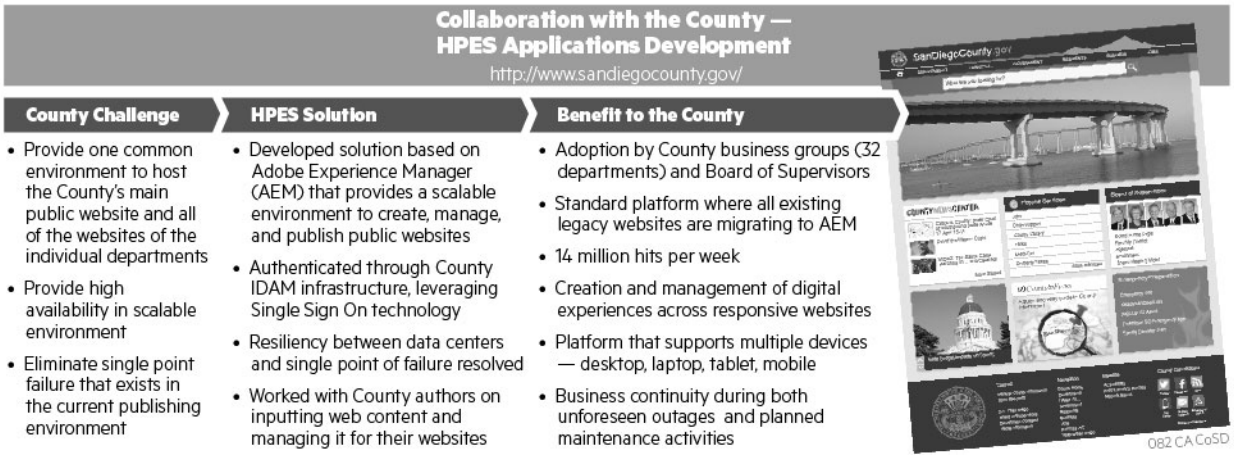
Our framework spans the full delivery life cycle.

Our application development framework is a delivery and governance framework covering all aspects of IT-enabled business change. The framework spans the full delivery life cycle, from application development planning through operations. Security is managed during the life cycle of the application, from discovery through operations.

Development Process

HPES' development processes will follow SDLC, using Agile, Iterative, and Waterfall methodologies as appropriate. For example, in 2014, our applications development team worked with the County to achieve a key IT initiative—a more public-responsive County web site, as shown in Figure 127.

Figure 127. Collaborating to Meet County Key Initiatives



We worked with County authors to develop the public-facing SanDiegoCounty.gov website, which was implemented in September 2014 and today gets 14 million hits per week.

Regardless of development methodology, each project will:

- Engage key stakeholders
- Identify the business, security and DR, and business continuity and planning requirements
- Analyze the requirements from internal and external perspectives
- Prioritize and select projects that will be included in the program scope.

For gathering and identifying requirements, HPES will leverage the Requirements Determination Process (RDP) that contains five major components: plan/manage, obtain, understand, validate, and evaluate, as delineated in Table 61. They obtain, understand, and validate components make up the core of the RDP. We execute these components multiple times, once for each set of requirements.

Table 61. Five Major Components – Requirements Determination Process

COMPONENT	PURPOSE/ACTIVITIES
Plan/Manage	We build the plan that we will follow throughout the process and manage overall execution of the RDP.
Obtain	We collect the information for the business, technical, security and DR, and business continuity planning needs of the County. We will store the information we obtain for later retrieval and traceability.
Understand	We will analyze the collected information to make sure we have a good understanding of the requirements. We then evaluate the statements for consistency, completeness, and appropriateness. For each statement, we will establish traceability and validation criteria and perform RCA.
Validate	We will confirm a mutual understanding of the implications of the requirements with the County and HPES SMEs, who will build and implement the solution.
Evaluate	We assess how well the process worked and determine the effectiveness of the techniques and the requirements statement. We will work with the County to prioritize the requirements and establish a roadmap.

During design, project details will be defined to align with the County's strategic direction.

Requirements are captured and more detailed views of the "As Is" and "To Be" states will be developed.

For existing applications, we will review the current state of the architecture and identify the impact of the solution as well as alternative solutions. We will notify the County of any changes that could impact the current architecture so a decision on solution options can be made early in the development cycle. HPES will also conduct industry research to identify any COTS product solutions that could meet the requirements.

The application architecture and its impact will be reviewed with the County to provide a better understanding of the changes and a solution design document will be created to document the solution with changes to the application, database and the infrastructure as needed. All design features as well as changes to data models and configurations will be documented. Detailed procedures to migrate data to the new data models will be defined.

Once requirements are defined, we will expeditiously notify external applications providers (The Select Group, SAIC, Apex Systems, CGI, TEKSystems and DVBE organizations, among others) and invite them to provide a bid for the work. This step, however, may not always be practical if available time does not support procurement activity.

After selection of an applications provider (HPES or a third-party), the provider will develop a detailed project along with an applications roadmap. The following describes various phases and deliverables of the project.

Deliverables for the assets and align phase include:

- High-level application solution design
- Application architecture
- Future roadmap
- High-level project plan.

When the project is implemented, the handover to M&O is executed to include documentation, training, and updated Service Desk scripts.

The project plan will include details of the application development, testing, integration, and implementation schedules. We will use our risk management processes to mitigate risks early in the process. We will provide detailed project and cost information to the County, and all changes to the plan and cost will follow the change management processes established by the County.

Figure 128. Apps Supporting County Citizens

Our applications development team adapted the Finding Rover app for County citizens.

Deliverables for the design phase include:

- Detailed design document
- Update architecture document

- Detailed project plan
- Risk and mitigation strategies
- Detailed project cost estimates
- Updated requirements document.

The develop phase produces the application code according to the application design. The primary deliverables are application code and test scripts and, when needed, a pilot run of the application. Key activities include:

- Application code development and test
- Gain authorization from the County to proceed to implementation.

For example, we worked with the County's Environmental Health Department and gained authorization to create a self-service Community Event permit site, as shown in Figure 128.

During this phase, the needed Dev/Test environments will be created. As new applications that are targeted to run in the MPC are developed, the HPES team will request MPC resources through the provisioning interface, including servers, software, storage, and backup requirements. Once the demand request is received by the system, and the automated parts of the provisioning process complete, the Applications team will then be responsible for installing, configuring, and testing each application component.

Conversely, as applications are retired or their Dev/Test components are no longer needed for live use, and therefore the associated MPC resources are no longer needed, the Applications team will submit a service request to de-install the MPC infrastructure for that application. The team will decommission all of the application components and infrastructure resources for the application environment being retired, and release any licenses through Asset and Configuration Management. If the environment is a Dev/Test environment, the request will specify whether the environment should be permanently decommissioned or put into cold storage. If the latter applies, the image will be preserved on the SAN storage and held in an online inventory, but its compute resources released. Otherwise, all resources will be released.

From a Resource Unit (RU)/billing perspective, only moves into and out of MPC for production application environments trigger activity: new RUs are added to billing at the point a production environment is made available for County use. RUs are removed from billing at the point when a request to decommission a production environment is issued and approved (the billing change does not wait for the decommission process to complete). If a production application moves from a traditionally hosted environment to MPC (as will be the case during transition), the old RUs are removed, and new ones take effect at the point when the MPC environment becomes available for County use. The County will not be billed for both sets of resource units. The same approach applies in reverse if an environment moves from MPC to a traditional environment.

Additions and removals of Dev/Test environments into and out of MPC trigger a slightly different RU action. Additions of new applications to MPC "draw down" on the pool of available resources. If the application is very large, such that its requirements exceed the capacity available (this scenario will be the exception rather than the rule), HPES may need to acquire more resources to expand the cloud. In most cases, the resources will be available, and the environments will be added with no change to RU billing. By the same token, removal of applications from the Dev/Test pool will not trigger a change to RU billing. Moves of existing Dev/Test environments into and out of MPC have no billing impact.

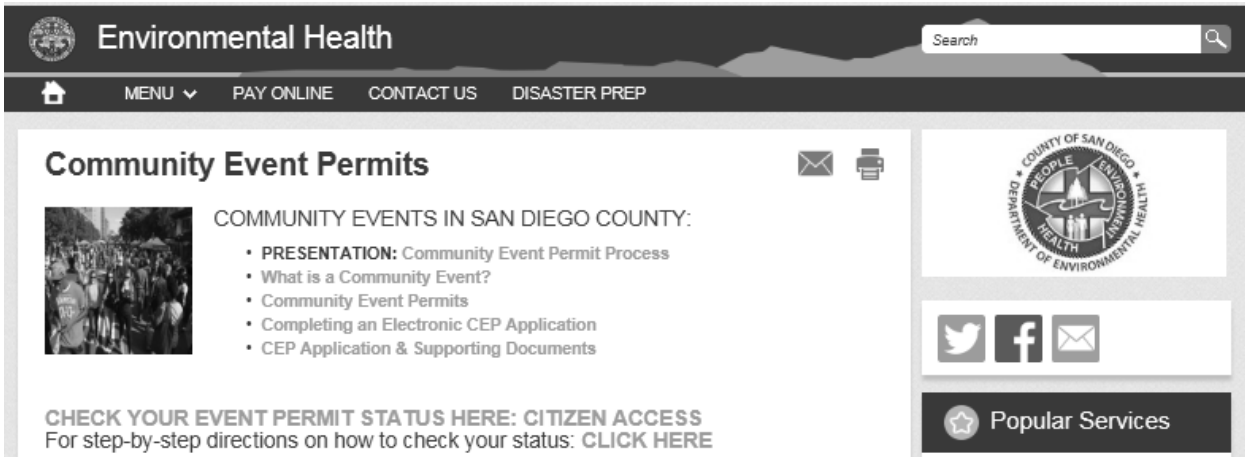
During this phase, application developers will implement the application according to the functional specification and application architecture. The developer will follow Software Development Lifecycle standard County process and standards to code, build, and deploy. The configuration changes will be documented and will become part of the deployment package. The technical lead will coordinate

integration testing with the developer in the development test environments. The designated testing team will also perform QA testing and user acceptance testing (UAT) and partner integration during this phase.

During the development phase, additional risks may be identified. Our PM will use the Risk management processes to mitigate these risks. Changes to the project plan and cost will follow the defined change management processes.

Our project manager will coordinate with the County to obtain approval for UAT and deployment to the production environment.

Figure 129. Creating Web Sites for County Residents



We developed self-service sites for County residents to facilitate their attendance at County events.

Deliverables for the develop phase include:

- Application code
- Test scripts, including test plans for the independent test team
- UAT results
- Risk and mitigation strategies.

HPES Continuous Improvement

HPES will make a business analyst available to the County to advise on cloud, mobile, and composite application processes that reduce deployment times, as discussed in Section 2.5.14. Our applications development team will be able to expand its use of Agile development techniques that drive improved delivery and County satisfaction.

Implement

After gaining the approval from the County using the successful UAT results, our deployment team will prepare the release package for deployment to production. A deployment plan will be created in coordination with the application users, the integration touch points and the M&O team. The deployment instructions including the configuration details and the data migration steps will be outlined and validated before deploying the application.

Deliverables include:

- Deployment Plan
- Deployment Package
- Third-party cross-training of HPES staff to perform required M&O activities, as required.

Manage

Once the application has been deployed in production, the project team will load all documentation, such as the architecture and design documents and the deployment package instructions, to the SharePoint DocVault site for the M&O team to review. An initial hand-off session will be provided to the M&O team so that the developers become aware of the changes.

The project team will coordinate and work with HPES resources to perform market research and technical trends, and provide new products and services and third-party solutions that may be applicable to the County. The team will work with the County to evaluate these services and make recommendations. The team's reach back into our quality management office will facilitate the process to provide recommendations on changes to SDLC, leveraging ITIL practitioners and their relationships with Software Engineering Institute (SEI).

High Level Requirements

Alignment with IT strategic plan and roadmaps: HPES understands the County's strategic plan and transformation roadmap and will make sure that all technology, innovation, reengineering, and business processes align. The development process will follow standards and guidelines published by the County's IT governance bodies and the architectures will comply with County-approved enterprise architecture(s), as well as abide by County security policies and models for system architecture and technology.

Our approach begins with analyzing requirements and constraints. Analysis of functional inputs will inform the business architecture view, which describes the high-level functional composition of the system and shows various actors, usage scenarios, and interdependencies among functional modules. After the first phase of high-level design is complete, the architecture artifacts will be submitted to County staff, as required, for review and approval. The outcomes of the review will be addressed by further aligning the architecture with the County's business and technology direction and resubmitted for approval.

HPES will recommend updates and revisions to architecture and/or configuration change designs in response to changing requirements, emerging technology, and other activities such as vulnerability assessments and performance analysis. Our team has the experience and skills to react to unanticipated changes and is ready to accurately calculate and manage the impact of specific solutions. HPES will also monitor industry trends and best practices and make recommendations to the County for other inclusions in the technology roadmap.

The software development process will follow the established SDLC process and generate documentation as required by the size and complexity of the project. As required, we will produce architectural design documents in compliance with the County's requirements and alignment with the County IT strategic plan and applications roadmaps.

Integration with existing data and Applications. HPES staff members have in-depth knowledge in the various applications codes and integration points. We know how these programs are related and will be able to quickly understand and develop the business requirements and resulting technical functionality as well as potential opportunities to offer further innovations.

HPES architects, engineers, developers, and operations support teams work in concert to facilitate new components introduced into the environment that are able to function as designed without negatively impacting existing systems or County users.

IT standards, guiding principles, architecture bricks and patterns. HPES follows all applicable standards and compliance requirements of the County and will maintain and support applicable CMMI, ITIL, and ITSM standards and industry best practices for the delivery of IT services.

Using our application development framework, HPES or a third-party will design the solutions for the requirements. We will follow County's IT standards, guiding principles, and architecture bricks. Any deviations will be identified early in the development cycle.

Planning and Standard Setting: For planning purposes, the HPES Program Office will provide budgetary estimates as required and follow standard change control procedures.

For standard setting, HPES will follow existing applications standards and work with the County to refine, improve, and modify as required. We will use our USPS Program Quality Office to validate best practices, tools efficiency, and process improvements.

System Documentation. HPES understands that the proper control, indexing, and maintenance of documents is vital to the software development process. Proper documentation enables developers to understand and identify the contents of software releases and location of components in a software baseline. HPES will continue to maintain the documents for the County program, with a sustained effort to improve timeliness and accuracy.

Cross-Framework Integration. HPES development framework promotes the identification of all dependencies, from internal and external applications or data, during the initial analysis of the requirements, during the discovery phase. All of the dependent applications, which are part of the impacted framework(s), are identified as stakeholders for developing the new requirement.

Once the new requirements have been identified, HPES staff will collaborate with the other framework teams to develop an interface control document, which will become the guide to perform the integration between the frameworks.

Our independent testing team will perform integration testing and, where possible, use service virtualization tools to test interfaces.

ITIL/CMMI Practices. HPES will operate the County environment using ITIL and CMMI best practices. The HPES ITSM community provides knowledge, best practices, and lessons learned to everyone supporting the County. We will leverage these unparalleled qualifications when bringing ITIL and CMMI-based processes to the County and recommend any changes to existing policies and procedures.

Standards

We will follow County's IT standards, guiding principles, and architecture bricks. Any deviations will be identified early in the development cycle and communicated to the County. HPES will follow existing applications standards and work with the County to refine, improve, and modify as required.

Application Integration and Testing

Application integration and testing are services associated with confirming that individual application framework components work together properly and, as a whole, perform their specified functions.

HPES will plan and develop our testing procedures to meet County requirements and policies. We will document the testing procedures in the Standards and Procedures Manual, including procedures to be followed by an independent testing team. HPES will develop an overall test plan for a release that includes the test strategy, coverage, scenarios, test bed, test data, methods, schedule, and responsibilities.

To effectively test an application, HPES will build and maintain an application Dev/Test environment that has been refreshed with production data. If necessary, we will build data masking programs to mask production data. HPES will build test cases to test the new functionality or components based on the

requirements and determine which valid data is required to appropriately test the application as well as the various testing phases. HPES will create a set of test cases to test the application end-to-end, new and existing functionality, application security and application supporting components, and infrastructure when needed. Benchmark test cases will also be created and run to properly execute regression testing. HPES will provide a reference to tie requirements and test cases together.

When testing an application, HPES will execute the test cases while following the standard testing procedures and verify that the test results meet County testing requirements. HPES tracks defects in a County-approved defect tracking tool and corrects retests functionality to validate repairs. In addition to testing the application HPES provides an UAT environment, if needed, that includes the necessary data. HPES supports the County in its UAT testing effort and provides access to the defect tool for entering found defects. HPES will assess and report potential risks to production of implementing a change and only implement after County approval.

HPES will manage the various Dev/Test environments including the application data, application releases, and supporting software and components. HPES stages the applications changes in the appropriate system in preparation for production implementation. We will support the production implementations, tracks the migration status of implementations and verify the implementation of changes into production. HPES defines the test-to-production turnover requirements and instructions for each project or release and will report the results, which will be shared with the County.

Data Migration

HPES will perform application integration and data migration, following the plan, build, and operate model.

HPES plans to create detailed plans for each implementation and migration that include the scope, approach and execution planned for the implementation. These plans will include "go-live" checklists, "go/no-go" meetings schedules and decision points, and intermediate "continue/rollback" decision meetings. All plans will include a rollback plan in case it is required. These plans will also include a communication section to coordinate the deployment with the County and other associated third parties. In addition, HPES will update any affected application documentation and production application support documents and procedures as needed.

HPES will perform each step in the deployment plan after receiving the necessary approvals. If the deployment impacts application documentation or production support, we will deliver updated application documentation and application support procedures.

HPES will execute, coordinate, and communicate with the County for all deployments and associated activities. For each deployment, we will perform all the needed steps of the SDLC such as requirements analysis, design, development, and testing. Our deployments follow the County's change and release management processes and are complaint with client change management policies. Documentation will be updated, including the Standards and Procedures Manual and Service Desk scripts. HPES will execute the deployment in production, once approved by the County, and synchronize in-production environments by deploying the implementation in the application's Dev/Test environments.

Application Training

Application documentation is defined as the conduct of all the necessary training programs for contractor personnel to preserve and enhance the knowledge and understanding of the applications.

HPES will develop plans to train new existing staff on the applications as necessary for new functionality and enhancements. When HPES builds an application release, we will update the application training plan as required.

During application operations, HPES will provide technical training and knowledge transfer to existing County support personnel, as well as materials related to the technical aspects of applications, as needed. HPES will develop, document and maintain the Policies and Procedures Manual, training, and knowledge transfer procedures that meet the County's requirements and policies.

Continuous Quality Improvement

Continuous quality improvement is defined as a systematic, planned set of actions necessary to for software development processes to conform to established functional technical requirements as well as with the managerial requirements of keeping the schedule and resources within budget. HPES will implement a process of improvement following the Action, Plan, Perform and Review model. This plan makes sure that customer requirements are met, risks and dependencies are managed, and existing resources are used. Development programs will be milestone driven and time-bound, focusing on quality and delivery targets. Outcomes will be reviewed jointly with the County for progress and benefit outcomes.

Application Quality Assurance (QA) Services

Application QA services is defined as a systematic, planned set of actions necessary to provide confidence that the software update/development processes conform to established functional technical requirements as well as with the managerial requirements of keeping the schedule and resources within budgetary confines.

HPES will create, update, and maintain a QA management approach for applications updates. This approach includes the following QA components:

- Quality management approach
- Effective software engineering technology
- Formal technical reviews applied during the SDLC process
- Multi-tiered application integration and testing strategy and implementation
- Control of software documentation and associate changes
- Procedure to measure compliance with software development standards
- Measurement of QA metrics and reporting mechanisms.

HPES will submit our QA management approach to the County for approval, after which it will be added to and kept current in the Standard and Procedures Manual.

HPES' determines QA metrics for each release and reports these to the County.

Transition. Our deployment plan will include a strategy to migrate the application into M&O services. After implementing the project in production, our development team will complete transition to the M&O team in an orderly, controlled manner that includes reviewing processes and outcomes, capturing lessons learned, and creating formal closure documentation.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Staff will be located at the HPES Rancho Bernardo office, El Paso, TX and Pontiac, MI.

- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

We will leverage Agile. Iterative, and Waterfall methodologies as needed for each project. The methodology selection will be discussed with the County and the necessary process will be executed based on the needs of each project.

As members of the PMI and ITIL communities, HPES provides training for resources, including acceleration programs for the PMP, CAPM, SPI, ITIL, and other disciplines. HPES participates in global, regional, and Community of Practice (CoP) groups, including the USPS PPM Community, State/ Local Government/Education (SLED) Community of Practice, and the USPS Business Analyst Community of Practice. In addition, we will monitor industry standards for emerging methodologies and discuss our findings with the County.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES plans to use the tools we are currently employing, such as HPE's ALM and Dell Marketing's Toad for Oracle software. We will evaluate other tools that can be used to automate application development services activities and make appropriate recommendations. We will evaluate automation in configuration and release management as well as the use of HPE cloud service automation and HPE Codar to bring in automation for release management and to integrate with server builds to implement DevOps capabilities.

Our applications development team uses HPES Project and Portfolio Management (HPE PPM) demand management module to centralize the resource assignment process. This allows us to strategically manage our workforce to meet the County's demand across the enterprise. HPES also uses PPM to track actual effort against project work, allowing quick access to level of effort information that can be used to inform decisions and prioritize work across all county projects. PPM also has a powerful workflow process engine that helps automate business processes.

- Qualifications and Experience – Background and experience in comparable environments

HPES has been performing application development for clients for more than 50 years and for the County for the past 10 years. We also performs application development for CDCR, which is responsible for the Strategic Offender Management System (SOMS). This integrated electronic offender management information system is one of the largest IT deployments in corrections in the United States. More recently, we have been supporting CDCR in improving their mobility application tools and providing a full range of applications development services including program and project management, and testing, our solution includes the following activities and tasks:

- Architect, install, and operate system hardware and software to support the application development life cycle (for example, development, testing, training, performance testing, production support, and production)
- Conduct system testing, performance testing, and integration testing of the solution
- Provide requirements elaboration and traceability
- Conduct design sessions to define customizations of the COTS offender management system necessary to meet specific needs of CDCR
- Develop web-based training and lead customer facing training sessions.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches *(optional)* – Submit a description of an alternative approach for consideration by the County, including rationale, trade-offs and potential benefits.

None.

2.10.1 Offeror Response to Application Services Specific Questions

2.10.1. Describe your organization's understanding and approach to meet the process and objectives for Applications Services described above, and any alternative approaches you propose for County consideration.

HPES has developed an M&O approach based on our knowledge of County applications, standard best practices, and review of several years of nondiscretionary data, specifically tasks and costs. Our approach will achieve manageability, efficiency, and quality while providing the County a cost-effective way to support your application suite.

Our fixed-price M&O Resource Unit (RU) includes preventive maintenance, application updates and patches (that do not involve new functionality or enhancements), continuous monitoring and fine-tuning for optimal performance, and, of course, all activities required to achieve restoration of service (i.e., break/fix). HPES will develop process improvements automation to reduce the cost of M&O services over time. All application patches for routine maintenance and/or restoration of services will include UAT.

HPES has assembled the County applications into 3 options/bundles where each options could possibility have 3 support models: full support, coordinated support and cloud-based Software as a Service (SaaS) support.

	Concept Considerations	**Concept Considerations**
By County	3 RUs (one for each bundle type)	Allocation to be determined/executed by County
By Business Group	15 RUs	Further allocation would be determined/executed by the County.
By Low Org	131 RUs	Assumes 47 depts., some may not have all 3 RUs. Low-org may be a better grouping as HHSA often uses a single low-org regardless of Dept.

Full support comprises a full range of application activities from Break-Fix incidents response, restoration of service, M&O activities such as installation of patch/upgrades for routine maintenance activities as described in Section 2.10. Full support includes those applications where HPES has the access and ability to affect change either with or without the participation of a third-party vendor

Coordinated support includes applications where HPES hosts the application but does not have security access or the ability to affect change. HPES will engage with the vendor and coordinate the necessary change(s). When possible**,** provided by 3rd party and approved by the County, M&O activities such as installation of patch/upgrades for routine maintenance activities as described in Section 2.10 will be performed

SaaS Support are cloud-based applications where HPES does not host the application and has no ability to affect a change. HPES will contact the SaaS provider and keep the County informed of the status of the issue or change.

On a quarterly basis—or more frequently if the County desires—HPES will review the Applications Portfolio with the County to evaluate the number of applications that have been added or retired and determine whether the RU warrants adjustment. HPES suggests that an ARB be formed to evaluate applications activity and provide go forward recommendations. The ARB will be made up of County and HPES representatives.

2.10.2. Your organization's proposed methodologies, processes, procedures and use of tools in new systems planning, SDLC, project management, testing (including methods to engage the County) implementation (including methods to engage the County), post-implementation evaluation/review and

transition (including transition support for newly implemented applications). Describe processes followed by your organization that minimize disruption to business operations.

HPES will partner with the County as part of a reliable, proven team that builds on our strong record of meeting County requirements, incorporating lessons learned, and continuing to develop, field, and support well-conceived, effective solutions.

Software Development Lifecycle Methodology and Processes

HPES will perform full software development lifecycle (SDLC) process activities for developing and implementing new systems and major scope enhancements to existing and evolving systems. Every software project has a unique set of requirements, challenges, and characteristics. HPES software development solution provides an agile, adaptable approach focused on delivering what is needed, not just the artifacts prescribed by a rigid methodology.

As a long-time County partner, our in-depth knowledge of the County's Applications Portfolio and business needs enables us to develop projects in alignment with County priorities. Our applications team supported the County in implementation of Key Strategic IT Initiatives outlined in the County of San Diego 2014 – 2017 Information Technology Strategy. For example, we worked with the County Board of Supervisors' staff to re-orient the County public website "to provide a more citizen-centric, platform independent experience," as shown in Figure 130. Throughout this document, we highlight collaborative success achieved with the County. HPES wants to continue to support fulfilling the County's Vision and Mission.

Figure 130. Innovation and Continuous Improvement: County News Center

Using a responsive Web design, the County connects today in a new way with its residents—in this case recognizing their dedication in supporting the goal of a safe, healthy, and thriving community.

Our applications team has experience in the development approaches used with the County and will comply with its governance and enterprise architecture principles as well as its procedures.

For each development project, HPES will work with the County's project sponsor or framework lead to create a project plan. The plan will detail the customized development approach to deliver the desired results with the best quality in the shortest time. We will employ proven development models that are widely practiced in the industry and that we have used previously at the County and on other successful projects. The alternative software development models lie on a continuum from very predictive approaches (requirements are well known, and the entire effort is precisely planned at the beginning) to

very adaptive approaches (requirements are not well known, and the requirements, plans, and solutions evolve over time).

In Table 62, we list software development models along with the general characteristics of each and the type of projects for which each model is best suited.

Table 62. Application Development Models

DEVELOPMENT MODEL	CHARACTERISTICS	SUITABLE FOR PROJECTS WHEN –
Agile	• Software is developed and tested in short iterations (1 to 4 weeks) • Adaptive • Iterations are usually time-boxed to limit risk • Software is the principal measure of progress, with less emphasis on intermediate artifacts • Face-to-face communication is preferred to documentation	• Requirements are not well known but can be evolved through short cycles • The project team is relatively small so that developers and customers can easily communicate and incorporate feedback into the next interaction
Waterfall	• Sequential process that flows through requirements capture, analysis, design, coding • Plan driven • Predictive • Low risk • Expected results clearly defined up front • Generally artifact intensive (models, plans, documentation)	• Requirements are well defined up front and changes are expected to be minimal • System reliability is critical • Documentation requirements are high • Project team is large and incorporates many disparate organizations

Our applications team adheres to County procedures that can be applied to Waterfall, Agile, or, alternatively, Agile/Scrum.

HPES is experienced in successfully employing development processes aligned across either development model shown as well as Iterative development, which lies in the middle of the development continuum. In the past few years, the County has employed the Agile/Scrum framework for application development. Scrum has proven very successful by including the County Product Owner in the development process to maximize the business value of the work performed, consistent with CoSD-295 Gate Review Procedure. Regardless of development process deployed, the following activities are common to nearly all projects:

- Business Modeling
- Requirements
- Analysis and Design
- Implementation
- Testing
- Deployment
- Configuration and Change Management
- Project Management
- Environment

Project Management

Overall governance of development projects will be managed by Project Management. Our ITIL-aligned project management methodology supports recognized industry standards, including the CMMI Institute's Capability Maturity Model Integration (CMMI), Projects IN Controlled Environments (PRINCE2), and the Project Management Institute's Project Management Body of Knowledge (PMI PMBoK) Guide. Our standard project management methodology provides the standards and rigor to support and deliver a high-performing team and high-quality IT services and is aligned with the County methodologies, processes, and specific RFP requirements, as described in Exhibit H.

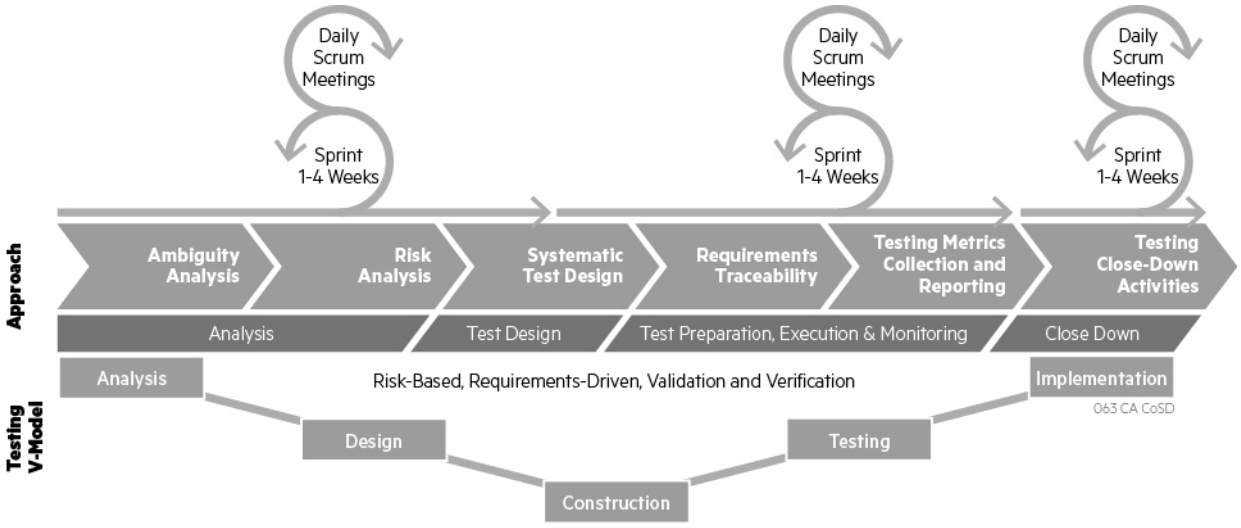
HPES uses a proven set of tools (like HPE's Project and Portfolio Management Center (PPMC)) to plan, budget, and track cost, scope, and schedule performance data. Our use of these tools, combined with our best practices and project management methodology, provides an accurate and responsive automated means to manage and track our performance. As our response to Section 2.10.4, we will engage the County in each step of the system development process—from evaluation to deployment.

As described in Section 2.6, HPES is rolling out a new Service Portal for the County that will provide transparency of our performance to the County. The Service Portal will provide access to the County on HPES service level performance, project schedules, and cost.

Testing

HPES will leverage the HPES Enterprise Testing (ET) Methodology to plan, develop, and conduct an integrated Test Program. The methodology will provide County visibility, traceability, and accountability in requirements management and verification; it will also provide risk identification, management, and timely resolution in support of the County development and maintenance activities, as shown in Figure 131. Our approach includes informal and County-observed formal testing to minimize software defect occurrences.

Figure 131. Testing Approach for County Applications



Our Enterprise Testing methodology accommodates our development cycles, maintains requirements traceability, and reduces risk upon project deployment.

As part of the HPE Quality Model, the HPE ET Methodology is driven by business requirements and business impact analysis in the early stages of an applications project, given this is where the majority of defects originate. Using our ET Methodology—a comprehensive framework that provides the structure, processes, tools, and templates—we will align to the County SDLC.

Our test team will conduct the Test and Evaluation (T&E) program, including managing the creation of test plans and procedures, testing, and developing test reports; communicate the result of testing and recommendations to the team and to the client; and provide input to our Program Manager on cost, schedule, and staffing for meeting requirements in this area.

We will prioritize high-risk, high-value business requirements and concentrate testing activity on those requirements to minimize risk and deliver the most value to the County for the application implementation. We will set the testing strategy based on the value of a business function as well as the potential for failure and the associated risk. The testing strategy applies the highest levels of test coverage to the highest-risk, high-value functions.

Our risk-based, requirements-driven testing has the following components, which can be executed iteratively:

- **Ambiguity Analysis –** We conduct an ambiguity analysis to make sure that the requirements document is deterministic (with randomness removed), unambiguous, correct, complete, and testable. We systematically analyze ambiguities in the requirements that drive application design, development, and testing to minimize inconsistencies and maximize requirements clarity.
- **Risk Analysis –** We systematically analyze risks in those requirements to reduce chances of misdirected or incomplete test coverage, with focus on isolating and mitigating the most critical risks first—those that most negatively affect the highest-priority aspects of an application or system.
- **Systematic Test Design –** Using methodical activities focused on managing and mitigating risks, we apply test design techniques to plan, choose, and develop the most effective tests to verify from the bottom up to integrated functional areas and interfaces within the complete system for operational configurations and environments.
- **Requirements Traceability –** Throughout test development and execution, we use a Requirements Traceability Matrix (RTM) to comprehensively depict test coverage and keep testing focused on high-risk, high-priority requirements.
- **Testing Metrics Collection/Reporting –** Testing reports offer ongoing insight into testing progress, coverage, and defect resolution; they offer timely opportunities for acting to mitigate risk before it causes irreversible harm.
- **Testing Close-Down Activities –** While testing ends with all tests executed, all defects resolved, and a system unquestionably ready for release, defects can outlast time and budget limits. We will focus on satisfying high-risk, high-priority requirements first through risk-based testing, leaving as the last priority tests and defects for only low-risk, low-priority requirements, as agreed upon in the Test Plan.

Our applications group uses the following tools from our Application Lifecycle Management (ALM) tool suite: the HPE Quality Center tool for test management and tracking, HPE Unified Functional Test for automated testing, and HPE Performance Center for performance testing. We use these tools to manage and develop a series of test scenarios and test cases that test the entire solution for functional and performance quality. Based on the broad scope of our testing and tools, we can use automated and manual test scenarios and cases to fully test the solution. We manage the test scenarios and cases with the HPE suite of testing products and then link and trace them to the approved requirements. Our approach sets the industry standard for testing software and results in higher efficiency and potentially lower costs.

Implementation

After Test, Installation, and Validation phases have been successfully completed, the implementation process continues with a final review of success factors, associated risks, and mitigation strategy. All of the primary technical functions will be documented and targeted, making certain that the applications development team and the County business owner agree with the decision to go to production. As

documented in the pre-application cutover phase, each functional area will be reviewed for completeness, functionality, and readiness.

HPES mitigates risks to integration of systems by applying our consistent, repeatable system integration and project methodology that provide effective communication, coordination, and collaboration with the County, which will result in a fully integrated solution. Key to the success of this process is continued collaboration through the County framework management.

We will develop a back out plan for each implementation to provide for rapid rollback to the original state if required. Whenever possible, the source system remains up and running until we are sure that the workload has migrated successfully. This approach provides a fully redundant contingency; immediately after implementation, our Applications Development team will test the functionality in the production environment to make sure County users will not experience any disruption.

Transition to Application M&O Services

After successful implementation, the applications development staff will provide support for the release. Within 2 weeks of implementation, our application M&O staff will receive cross-training and documentation to provide a smooth transition from development to M&O. The development staff will also review with the O&M staff any changes to the design and deployment document as well as the test results.

2.10.3. Your proposed application demand management methodology.

An objective of the County's 2014–2017 Information Technology Strategy is a consistent approach and improvement across the portfolios through oversight of key projects and initiatives. Our ITIL-aligned demand management methodology uses frequent communication with the County Technology Office to maintain alignment with the County's strategic priorities and schedules for new or modified application deployment.

Business analysts (BAs) will assist the County in identifying and prioritizing future demand. Embedded with County departments, BAs will work closely with the County users to understand and articulate business needs to the CTA. In turn, the CTA will work with the technology office to determine which technologies may be required to meet the business need. From that determination, the Applications team will forecast demand by department, technology, and timeframe.

Additionally, future demand will be triggered via workshops, enterprise roadmap development, and strategic planning with County departments.

The HPES application demand management tool—HPE's PPMC Demand Management module—has proven crucial to our application demand management methodology for County projects. HPE PPMC consolidates, prioritizes, and fulfills the strategic application projects activities so the County can redirect activity based on demands.

The PPMC tool lets us consolidate and prioritize the applications requests and focus on the highest-priority County initiatives. For example, HPES responded to the County's request to work with the Office of Emergency Services to create a responsive new website notifying residents of emergencies in multiple languages as well as describing how to prepare for them and how to recover, as shown in Figure 132. We have equipped the site with a Wildfire Hazard Map tool and provided wireless access to emergency alerts via mobile phones.

Figure 132. Promoting Safe Communities

We collaborated with the Office of Emergency Services to meet the County's key IT initiative for a responsive public website for residents (and their pets) in case of emergencies.

Because the PPMC Demand Management module captures all IT requests, it enables County stakeholders to have a comprehensive picture of past, present, and future IT demands, grouped by demand category.

The PPMC Demand Management module processes a request based on the best-practice process and business rules for that type of request, after each request is captured. The process behind each request is modeled, automated, enforced, and measured. Automated, out-of-the-box, best-practice processes—including proposed projects, application-related enhancements, project scope change requests, non-project related requests, and others—are easily configured to support the County's specific best practices, using a drag-and-drop process modeler.

The module helps responding to new demands and changing priorities by redeploying resources and provides the automated processes and data necessary to effectively manage status, service levels, and trends. Web-based dashboards provide real-time visibility into request status, priority, next steps, and summary views. Service levels are updated automatically as each request is processed.

Business rules define when to send notifications so the PPM module can monitor processes in real time and alert the County and our applications team when something needs attention. Flexible reporting makes it easy to identify trends across request types, response times, escalations, and priorities to help focus IT resources appropriately.

When priorities change, cycle times may be exceeded, or other requirements possibly may not being met, PPM can trigger an escalation process. With this level of visibility and control, we can focus on the highest-priority requests and know quickly whether a project may be in jeopardy.

How HPE PPM Demand Management Works

Each request type has an associated workflow, which specifies the process for reviewing, evaluating, prioritizing, scheduling, and approving the request. Based on the workflow, the reviewer can assign the request to a person or team for scheduling and delivery. Notifications defined as part of the process can be activated at any step to indicate work that needs to be done, has not been done, or is being escalated.

With online access, managers can assign tasks, and developers can view and work on tasks assigned. Service levels are updated in real time, and changes are captured for a complete audit trail. We will link the module to the new Service Portal described in Section 2.6. Key features and benefits of PPM Demand Management are as follows:

- **Shared demand repository**: Consolidates and stores application demands for better reporting, visibility, and control
- **Unlimited demand categories**: Configures demand categories, such as business application initiatives
- **Demand scheduling and prioritization**: Lets the application services team schedule requests by priority, date, contribution, or other metrics and enables adjustment of priorities to reflect current or expected business needs
- **Drag-and-drop process modeling**: Allows County procedure rules, out-of-the-box processes, and creation of new processes in minutes to meet specific business needs
- **Complete audit trail**: Captures every change to every application request for a complete, detailed audit trail

2.10.4. Your proposed approach for performing system analysis and design for major new development projects and enhancements. Describe how you expect the County to be involved in the analysis and design process.

HPES will work collaboratively with the County during the planning, analysis, and design phases of development projects. Our approach includes the following activities that we will perform iteratively throughout the delivery life cycle. We will adhere to the CoSD 295 Project Gate Review Procedure applicable to all applications development projects. We outline the Gate Review Process in Section 2.10.6.

Collaborative Planning with the County – Analysis and Design

Upon receipt of an approved request, HPES will kick off the project by conducting a series of workshops with the County project sponsor. Our team's focus during the planning workshops is to facilitate collaborative dialogue with the County on design of the new system. Our expectation is that the County product owner will describe the intended result so our team can understand the requirements, begin to design the architecture, and apply the appropriate technical standards.

During these workshops, we will discuss "user stories" that encourage the County to visualize the new system as deployed. Analysis of the new system will include realistic assessment of anticipated improvements, potential limitations, and possible risks. Looking forward, we also will discuss system business rules needed to facilitate continuity from the existing process to the new system. We used this approach in planning the responsive web app shown in Figure 133. We will build a roadmap and next steps with the County that sets realistic target dates for solution design, development, testing, and deployment. The roadmap will define the County's role throughout the development process.

Our approach allows the County to continue to provide design input throughout our iterative processes, keeping the new system development aligned to County objectives.

We will maintain SDLC documentation as the project progresses. This includes documentation of the County's priorities, the solution design and its characteristics and features, results of the collaborative analysis including risk assessment, and the improvements anticipated upon deployment and all approved changes. Based on the planning workshop discussions, our team will refine and document the functional and nonfunctional technical requirements and submit them for County approval.

2.10.5. Your proposed strategy with regard to cloud and E-commerce solutions. Describe your experience implementing E-commerce and cloud solutions for other government customers. Describe your proposed methods to ensure that such applications remain secure.

Figure 133. Meeting the County's Strategic Initiatives – Beach Water Quality App

085 CA CoSD

Working together with the County Department of Environmental Health, we developed an app that provides water quality alerts on 80 beaches in San Diego County that residents can view on their mobile phones, iPads, tablets, or desktops

Cloud Services

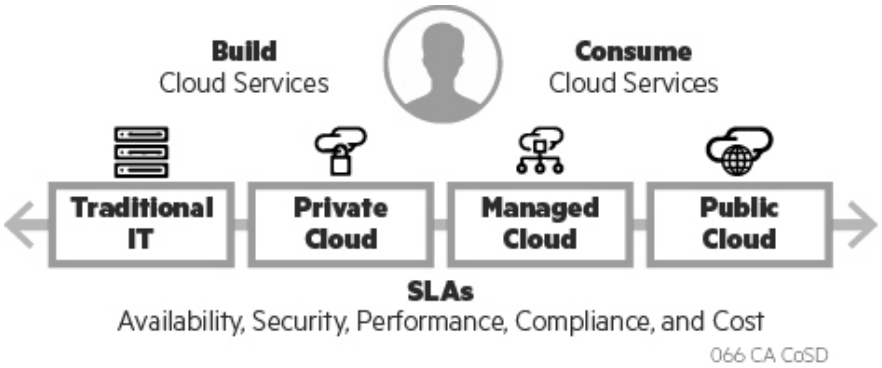
As a global leader in cloud services and technologies, HPES has been delivering compute services in a utility, pay-as-you-go model for more than 10 years—before advent of the term "cloud." With the planned consolidation to the Tulsa data center, HPES will take this opportunity to move the current dev/test application infrastructure from a well-performing traditional hosted environment to a more agile, hybrid Managed Private Cloud (MPC) for compatible platforms, and retain the traditional hosted environment where necessary for applications that are not initially cloud compatible. The MPC environment is a highly standardized environment with high redundancy and high availability for both infrastructure and applications to eliminate single points of failure. Moving to MPC preserves the benefits of the current environment and uses streamlined server provisioning, enabling HPES to provision, scale, and de-provision virtual servers in hours instead of days. It also includes tools that simplify capacity and performance management, monitoring, patching, and security and regulatory compliance and provides the foundation for the County to take advantage of additional public cloud services. HPES will work with the County to identify production applications that are candidates for the MPC environment.

In partnership with AT&T, we have already rolled out several virtualized services for the County and have more planned in the coming years. In Section 2.8, Network Services, we describe how we are positioning the County for cloud-based software-defined networking. Our proposed network is designed to provide maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest security and service levels. Acting as an "enabler to the enterprise," our proposed network will enable any device—managed or unmanaged—to be evaluated, authenticated, and allowed policy-based access.

HPES MPC approach leverages HPES cloud resources expertise coupled with knowledge of the County's environment; best practices; and standard functionality, integration, and automation.

Our solution's user-friendly portal will result in quick adoption, and provide state-of-the-art software for cloud service catalog presentation, automation, management, and orchestration. HPE's Cloud Service Automation (CSA) Portal platform is the user entry point into the Cloud Consumer Portal. Users can view service details and subscriptions through an easy-to-use self-service portal.

Figure 134. Full Suite of Cloud and Cloud Broker Services



As builder for some, broker for all, HPES offers a complete suite of Cloud and Cloud Broker Services. In addition to HPES MPC, we can place workloads with Azure, Amazon Web Service, or any qualified vendor. The decision regarding which vendor to use will be determined by the application requirements including volume, access, dependencies, and security.

HPES' cloud solution enables delivery of IT resources as "services"—such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—to consumers using ITIL-based management and operational support processes through a web-based, private Cloud Consumer Portal. HPES skilled resources provide setup, configuration, and ongoing management of the private cloud, so applications development staff can more effectively complete projects.

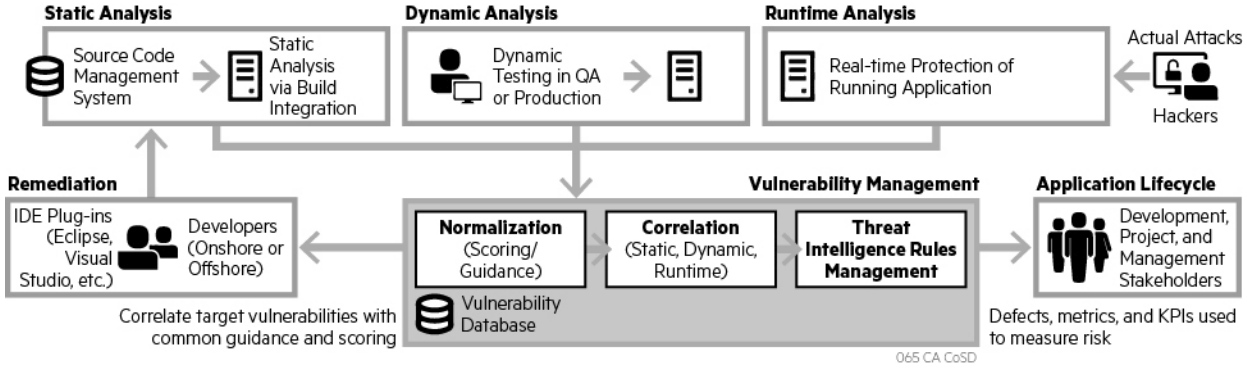
HPES Cloud System enables our development team to build and manage services across private cloud environments on a simplified, integrated architecture:

- Intelligent automation; application-to-infrastructure
- Complete service life cycle management—from provisioning to monitoring to retirement/de-provisioning
- Supports multi-hypervisor, multi-operating system (OS), and heterogeneous infrastructures – now including Kernel-based Virtual Machine (KVM) and Hyper-V support
- Pre-packaged service design tools – HPE Cloud Maps, which are pre-configured and standardized workflow templates for infrastructure deployment, application deployment, and life cycle management; HPES has invested and developed more than 200 HPE Cloud Maps for leading independent software vendor (ISV) solutions from Microsoft, Oracle, IBM, Tibco, Citrix, SAP, Red Hat, Symantec, and more
- Out-of-the-box bursting capabilities broker service delivery across multiple clouds from a single, integrated point of control
- Built on proven and market-leading HPE Converged Infrastructure and HPE Cloud Service Automation (CSA). Combined with Operations Orchestration (OO) and Matrix Operating Environment, CSA automatically enables the design and provisioning of virtual infrastructure services in hours instead of days. HPES Server Automation software enables us to automatically perform activities such as server discovery to provisioning, patching, configuration management, and script execution to comply with HPES IT configuration standards.

Security

HPES is one of the top contributors to the OpenStack community. Our cloud solution provides capability to perform Static Code Analyzer (SCA). This service focuses on implementation of the Static Analytics, Remediation, and Vulnerability Management of the architecture in the Figure 135.

Figure 135. Essential Building Blocks of a Mature, Secure SDLC for Cloud Services



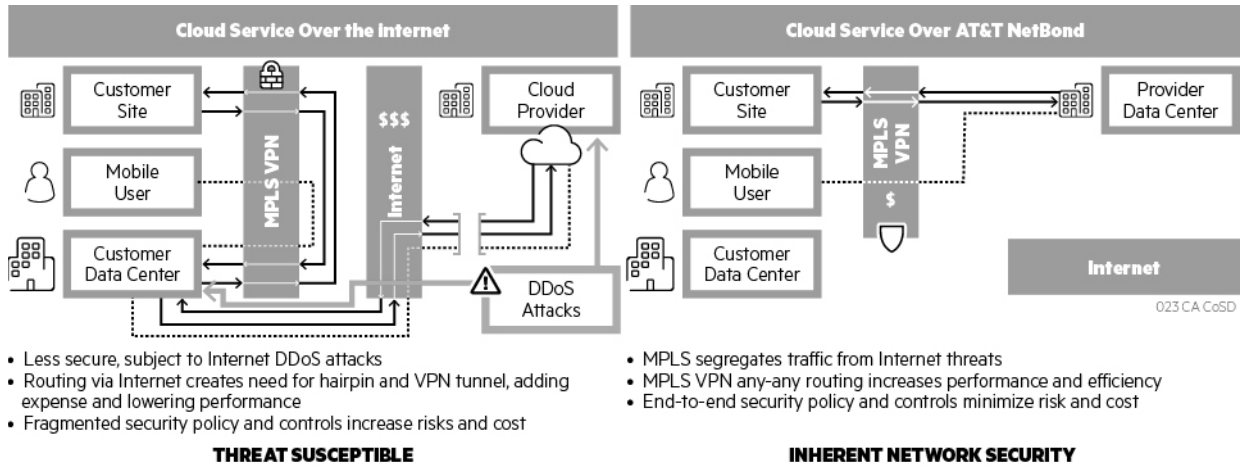
HPES will provide a, short-track implementation into the County environment that will result in a scan of the target application. This will enable our team to accomplish the following:

- Produce SCA scans
- Triage scans results to identify and prioritize security vulnerabilities
- Incorporate the HPES solution for the County into the development process

Embedding our solution within the software development lifecycle enables secure development practices and keeps applications protected from external threats.

In the background, our network security is built on AT&T cloud security, described throughout Section 2.8. Figure 136 shows the difference in risk between a typical Internet cloud solutions as compared to AT&T NetBond as a basis for cloud services for the County.

Figure 136. Cloud Service over AT&T NetBond



We avoid the security risks of the typical cloud service over the Internet by providing end-to-end security with NetBond.

HPE Cloud Service Automation (CSA) goes beyond traditional IT provisioning; it increases agility and reduces costs. This solution offers the following:

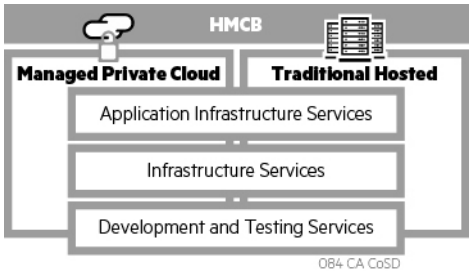
- Leverages a modern, easy-to-use self-service portal with an intuitive shopping cart experience for ordering infrastructure and application services across both private and public cloud environments.
- Enables an open, heterogeneous, and extensible architecture supporting OpenStack-based cloud standards, with multi-hypervisor, multi-vendor hardware support that avoids the pain of vendor lock-in.

- Embraces existing automation assets in a highly automated cloud lifecycle management platform that uses an enhanced orchestration engine.
- Designs and orchestrates full-stack services with topology service designs for faster time to value
- Stages complex multi-tier applications with sequential service designs
- Gains enterprise-grade service management with a highly available architecture, providing informed, transparent IT service delivery for secure and compliant services.
- Creates an IT service control point, enabling hybrid IT management across the expansive HPE Helion portfolio of private, public, and hybrid cloud services.

In solving the problem of demand, another problem has emerged: how to efficiently manage resources and services that span private and public clouds as well as traditional IT. Until now, the processes for managing service provisioning have generally been manual, inefficient, and solid. Such time-consuming and therefor costly processes create a drag on IT and result in less innovation and less agility in the face of changing business requirements.

The key to efficiently managing hybrid delivery using HPE CSA for cloud management is shown in Figure 137. The proposed solution features an open, extensible architecture that supports HPE and third-party management tools, enabling us to quickly adapt to changing business requirements while supporting heterogeneous IT environments.

Figure 137. HPE Cloud Service Automation (Cloud Brokering)



HPE Cloud Service Automation will enable us to broker and manage private cloud, public cloud, and traditional IT services for the County.

E-Commerce Solutions

HPES offers a number of E-Commerce Industry-focused solutions, depending on the type of transactions or services the County desires. Because these cannot be priced without specific requirements, they have been removed from the proposal at the County's request. An example of implementation for another client is provided below per the RFP requirement.

Industry Example – Government Healthcare: We are the nation's largest provider of Medicaid and Medicare process management services, administering $140 billion in benefits a year. We serve as the fiscal agent or principal IT provider for Medicaid in 19 states. Our U.S. healthcare experience spans payer, government and life science communities.

We bring nearly 40 years of experience in healthcare information technology and have worked with groups such as commercial healthcare plans, the U.S. Department of Defense Health Affairs, disease and care management organizations, Medicaid, and Medicare. In addition, HPE was intimately involved in developing e-commerce standards for the industry and held key positions with leading industry organizations:

- Accredited Standards Committee (ASC) X12
- National Council for Prescription Drug Programs (NCPDP)
- Health Level 7 (HL7)
- Healthcare Information and Management Systems Society (HIMSS)
- Health Committee of the U.S. Chamber of Commerce
- American Accreditation HealthCare Commission/URAC
- Workgroup for Electronic Data Interchange (WEDI)

Cloud Implementation Experience

In support of multiple Department of Homeland Security (DHS)-wide initiatives, a cloud-based SaaS solution has been deployed using the Microsoft Dynamics CRM platform. This SaaS offering deploys and scales business operations such as records management; scheduling; reporting; tracking campaigns, mission, and workforce activities; and budgets. Within the DHS, Microsoft Dynamics CRM is used by the Transportation Security Administration, Federal Emergency Management Agency, Customs and Border Protection, Immigration and Customs Enforcement, and U.S. Coast Guard.

2.10.6. Your organizations approach and experience in leveraging waterfall and agile development approaches for an organization and portfolio such as the County's.

We will use Waterfall or Agile approaches based on best fit for the project. We have successfully implemented development with both methodologies for the County.

Waterfall Approach

In Waterfall life cycles, each phase (Define and Analyze, Design, Build, Test, Release, and Deploy) is typically executed sequentially, possibly with overlap but with little or no iteration. HPES will use Waterfall life cycle development for projects that require a Waterfall approach to deliver business applications or to implement major application enhancements for an existing system. This approach emphasizes up-front requirements and design activities and produces documentation during early development phases. This approach should be used when requirements are clear and stable because the amount of re-work can be considerable if changes occur in requirements during subsequent stages of the development life cycle.

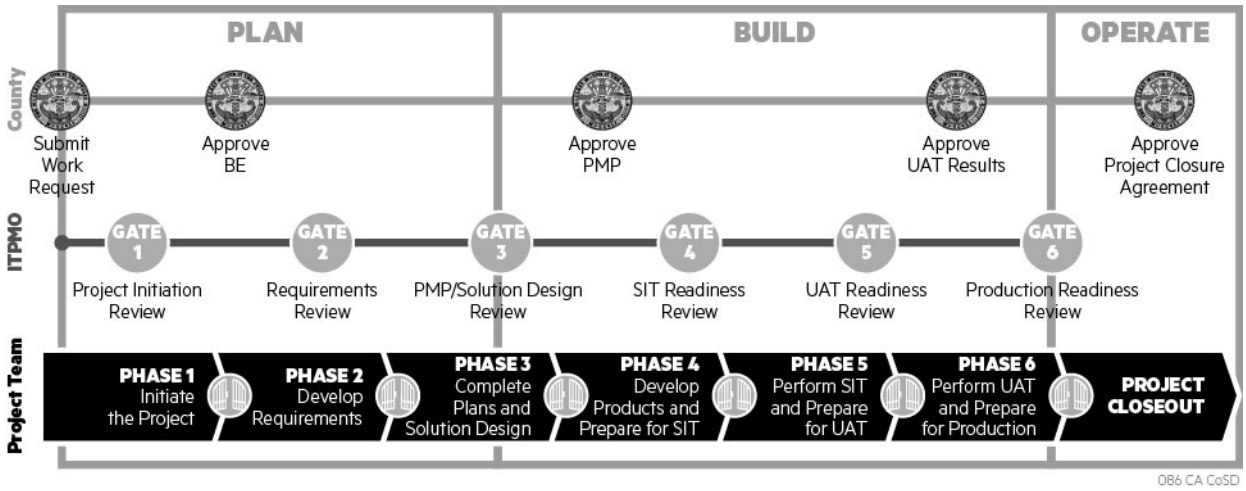
The HPES Waterfall approach used at the County consists of various phases, Waterfall steps and approvals, and checkpoints, as depicted in Figure 138.

Agile Approach

Many business initiatives or problems are best solved through an adaptive, incremental exploration of the solution domain, using inspection and adjustment in a cycle of continuous improvement. Rather than fully specifying a solution up front, change is embraced and the solution is grown to best suit the needs of the user community, maximizing value delivery while optimizing TCO.

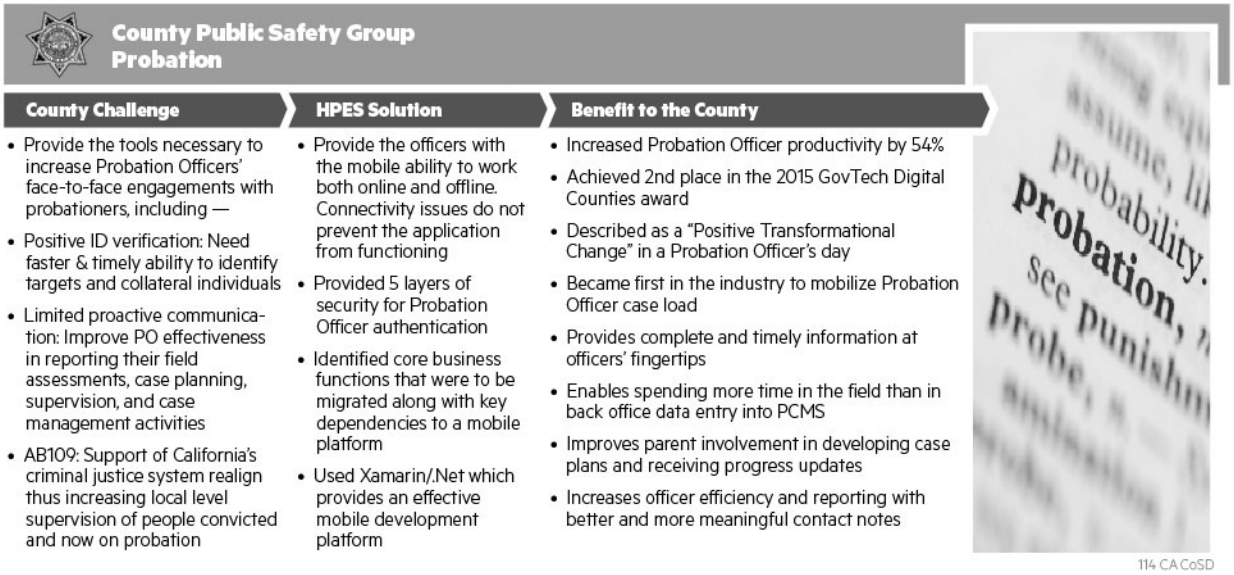
In situations that call for lean software development, HPES tailors an Agile development approach for each project. Based on the Scrum framework, this approach uses an appropriate selection of sound engineering practices from Extreme Programming (XP). It provides a substantial benefit by enabling rapid scalability if required, taking advantage of teams working concurrently in multiple locations, while preserving the ability of rapid response to change. We developed the County Public Safety Group Probation application (PUMA), shown in Figure 139, based on Agile principles.

Figure 138. The County's Waterfall Methodology and Gate Review Approach



Our applications development team involves the County Product Owner and project stakeholders in all of our development efforts.

Figure 139. HPES developed the County Public Safety Group Probation application (PUMA)



Scrum Framework

The Scrum framework is used throughout the applications industry for everything from simple projects to changing the way entire enterprises do business. Scrum significantly increases productivity and reduces time to benefits while facilitating adaptive, lean systems development.

Based on modern empirical process control theory, Scrum supports a work process that optimizes the quality and level of functionality of products and solutions that can be created in a given period of time, given available resources, as agreed upon by the County. Useful product functionality can be delivered timely (such as every 1 to 4 weeks) as specifications, architecture, and design emerge and transform into working software, even when working with volatile requirements sets or technologies.

Scrum is an iterative, incremental framework for projects and product or application development. It structures development in cycles of work called sprints, which may range from 1 to 4 weeks in duration.

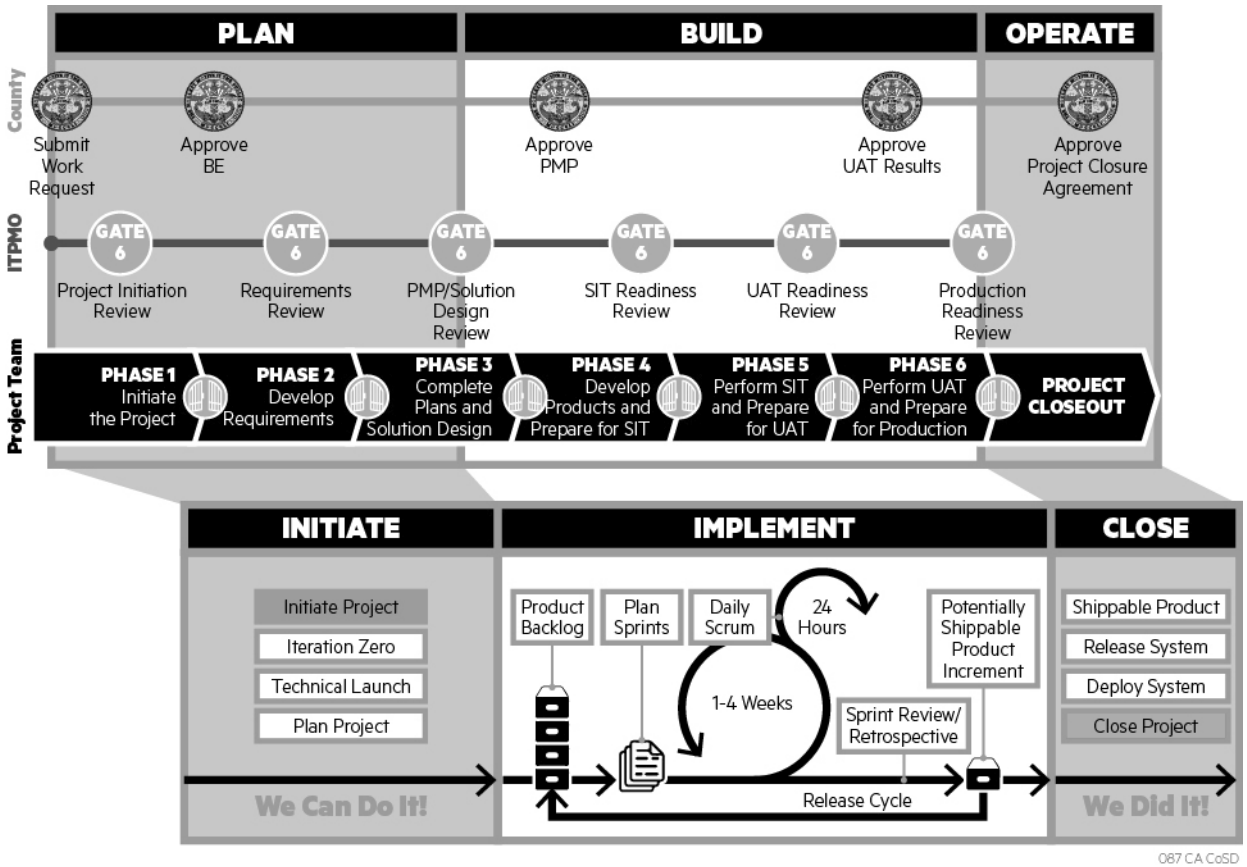
The sprint length is usually consistent over the course of the project, and sprints follow one after the other without pause.

Work begins as the County product owner articulates the product vision and puts together a product backlog that contains a set of high-level features to help realize that vision. At the beginning of each sprint, the integrated team selects items (specific features, user stories, customer or architectural requirements) from the product backlog, which has been prioritized under the direction of the County product owner. Selected product backlog items are then elaborated such that they are ready to be fully estimated. The aim is to fill up the sprint backlog up to the known capacity of the team—the team velocity.

The team and the product owner agree on a mutually agreeable definition of "done" for product backlog items. For example, in the case of software, this means code that is integrated, fully tested, and potentially deployable, including any necessary installation, documentation, and training updates. Based on this definition of "done," the team commits to fully complete the sprint backlog items by the end of the sprint.

During the sprint, chosen items do not change. Every day, the integrated team gathers briefly to inspect its progress and adjust the next steps needed to complete the work remaining. At the end of the sprint, the team reviews the sprint with stakeholders and demonstrates what was built. Ongoing feedback identifies problem areas, and relevant countermeasures are designed and incorporated into the next sprint, in a continuous improvement cycle. Figure 140 applies the County Waterfall gate reviews to the Agile development process.

Figure 140. Using County Waterfall Gate Reviews with HPES Agile Development Process



We maintain County procedures during our Agile/Scrum development.

Experience

Waterfall. To meet New Mexico Public Employee Retirement Association's (PERA) objectives, HPES implemented the Clarety Pension Benefit Administration Framework to handle all employer and member pension administration business functions. We delivered Clarety for NM PERA's Retirement Information Online (RIO) solution. Membership was implemented using traditional Clarety Waterfall Systems Development Lifecycle (SDLC) methodology by conducting gap analysis, collecting detailed requirements, developing use cases, and obtaining signoff. This was followed by detailed design and development activities and system testing.

Agile. In addition to the County projects mentioned above, HPES is the primary integrator of the State Tax and Revenue System (STARS)—the principal system of record in Ohio for tax filing, billing and collections, revenue accounting, overpayment and overdue processing, taxpayer information queries, information to counties, and management of correspondence to taxpayers. HPES was tasked with integrating Ohio Department of Taxation's (ODT) 27 tax administration systems into one platform. We worked with ODT to develop, test, and implement the solution. HPES has supported ODT in diligently working with its tax business leaders and IT project team to take advantage of technology that enhances the agency's mission and goals. This task required intense involvement of business leaders, fostering the right culture, and teaming with vendors. An integrated team consisting of ODT business users, developers, testers, business analysts, and system administrators was critical to the success of this project.

2.10.7. Your proposed approach to deliver End User training, including the location and method of training, frequency of training, and documentation provided with training.

End-user training spans the spectrum from low-touch online training or videos to specialized in-person classes or seminars.

For low-touch training requirements, HPES will develop online training appropriate to the projects. This may include Adobe Captivate vignettes, videos, or posted documentation and frequently asked questions (FAQs).

For specialized in-person training, the County currently uses the 200-square-foot HPES/County training center in our Rancho Bernardo location. We will continue to maintain and make that space available to the County. The center provides 36 County-imaged desktops hosted on the County of San Diego Network and provides a quiet, controlled environment. The center's simulation environment accommodates User Acceptance Testing (UAT), which allows the County to test features and functionality prior to deployment.

The facility has printing and projection capabilities to support a successful training experience. This facility will continue to be available as well for County trainers to train County staff.

Our objective is to provide the right kind of training at the right time. Major releases may require online and classroom training for the user community on a scheduled basis, while minor changes may require only an update to procedures or processes and notification to the user to use the new process.

In addition to training users, HPES will conduct new and refresher training programs for our personnel to preserve and enhance the knowledge and understanding of the applications and the underlying technologies and frameworks on which they are built. The training includes industry standard certification as well as external training on the latest releases of databases, middleware, enterprise platforms, and applications as required.

HPES will train our development and M&O staff to support application development and changes when implemented into production. We will follow ITIL-aligned processes for training documentation.

Additionally, HPES will develop and conduct cross-training to facilitate smooth transitions between HPES personnel as required and to make sure backups are in place for each application.

2.10.8. A statement of whether or not your organization will follow the current County processes for completing in-progress projects. If not, explain your approach and describe experiences your organization has had applying your methodology to in-progress projects.

Yes. HPES will follow current County processes as we complete in-progress projects.

2.10.9. Provide references to organizations similar to the County where your organization has performed Business Process Re-engineering (BPR) services, including specific examples of productivity gains and service delivering improvements achieved by other clients in implementing your strategies.

We offer three examples of other clients for whom we have supported or provided BPR efforts as follows:

- Navy
- Defense Information Systems Agency (DISA)
- Department of Housing and Urban Development (HUD)

Navy

Under the Department of Navy (DON) Selection and Classification (RIDE Web Services, Fleet RIDE Development, Deployment, Sustainment, and Enhancement) contract numbers N00189-07-D-Z015 and N00189-11-D-Z019, HPES reengineered three major mission processes for the Navy, and then deployed the enabling technology to allow the transition to production operations.

- Reclassification at Navy training sites
- The ratings process
- Perform to Serve (PTS).

Navy's Move to New Processes and Systems

Mission Process 1 – Developed Chief of Naval Operations Instructions to more clearly define Reclassification Policies and Production Management Office overarching guidance.

Mission Process 2 – Redesigned and implemented an improved process, supported by an enabling IT system (Fleet RIDE), to vector top-performing, undesignated Sailors to careers in the Navy's undermanned ratings.

Mission Process 3 – Reengineered Fleet RIDE to integrate the Navy's Perform To Serve (PTS) program functionality within Fleet RIDE.

Results:

- Achieved 24% increase in program compliance (from 74% to 92%) since 1 October 2010 deployment
- Reached 25,000 re-enlistment applications per month, a 150% increase over the legacy system
- Allowed the Navy to retire the legacy PTS system while improving efficiency and effectiveness

DISA

The DISA Computing Services Directorate (CSD) awarded HPES contracts for the Special Processor Environment (SPE) solicitation through which they provide on-demand processing capacity, storage, software, content delivery services, and professional services (labor) as a managed service. Our cloud environment for DISA consists of a Rapid Access Computing Environment (RACE) that allows DISA customers to provision test and development environments quickly for a basic monthly fee.

We provide compute capacity as a service as well as capacity management and planning, and architecture design for new applications. We also provide Software as a Service (SaaS), Storage as a Service (STaaS), and Infrastructure as a Service (IaaS). Our cloud solution provides HP-UX, Microsoft Windows, Red Hat Linux, SuSE Linux, VMware, and all supporting hardware and software on-demand, priced as a utility offering within time frames ranging from immediate provisioning to a few days for complex environments. The scope of our offering accommodates new business and migration of current workloads as refreshment of the technology base dictates.

The services our computing cloud provides are similar to the County's Framework Services. They include operating environment and server administration, virtual machine management, database administration, configuration management, service desk, information assurance support, and network integration support. The DISA cloud consists of modular, scalable, low-cost commercial off-the-shelf (COTS) IT capacity and the ability to manage and provision virtualization software, processing capacity, storage components, networking interconnects, operating systems, and management software. It provides a powerful workload orchestration and management software integration that enables scheduling, advanced policy management, and tools to control all components of the cloud resources and IT infrastructure.

DISA's Move to On-Demand Computing

Mission Process 1 – Helped DISA move its computing and applications testing environments to a demand-based services model.

Mission Process 2 – Helped educate DISA's DoD agency customers about the new services and how to acquire them.

Results:

- Shortened acquisition timelines for processing capacity from a previous 6 to12 months to 14 days
- Reduced costs by deploying low-cost and virtualized blade systems for DoD applications and consolidating, by a ratio of 8 to 1, many physical servers into fewer ESX physical hosts
- Increased security. HPES is the first solution provider to design, build, deploy, certify, and manage a cloud computing solution on the classified DoD network

"The management of this contract has met or exceeded expectations…This contract is one of the smoothest running I have worked on for the size and complexity of the contract… I was responsible for monitoring, assessing, recording and reporting the technical performance of the Contractor on a continuous basis…I found HP's performance to have been exceptional in all areas."

Helping HUD to Modernize Its Systems and Processes

Implementing a roadmap for change HPES' design took HUD from inflexibility and lack of integration to integrated, standards-based services. HUD now has a very agile, responsive, highly available, scalable IT environment that runs its legacy applications and allows HUD's next-generation web applications to go live on time and successfully.

HPES re-engineered HUD's server environment, established the first large-scale Government private cloud, and is currently establishing a multi-cloud managed environment. Our HUD Information Technology Systems (HITS) program is certified at ISO 20000 quality standards and is firmly founded on ITIL-based processes. We have conducted more than 10 technical innovation forums to introduce new technologies or concepts for HUD's consideration.

2.10.10. Your proposed diligence and analytic process to determine how to carry out Applications M&O Services work on a fixed price basis by application bundle. Include the following factors in your response:

2.10.10.1. Methodology and analytics used to assign an Application to a fixed price bundle

With more than 6 years of Non-Discretionary Work Request (NDWR) data, HPES determined usage by percentage by Business Group. The estimating method defines a basic process that HPES follows and is intended for use with the HPE Project Management Methodology.

For the County, we used the bottom-up approach for application M&O estimation. The process consists of the following steps:

- Identify domain(s) of applications
- Gather historical information such as non-discretionary work orders

- Determine application size, complexity, and environmental characteristics
- Develop application bottom-up estimates
- Identify required infrastructure

To facilitate estimation of the County Portfolio Applications transitioning from a Time & Materials (T&M)–based contract to the Fixed-Price contract, we used our Inventory for Client and Agency Planning (ICAP) tool, in which we entered all of the application parameters. The tool provides us with a model for determining what it needed to perform the work in a Fixed-Price mode. Next, we reviewed the numbers with our account and delivery teams to verify that all considerations and constraints were addressed that could impact the service in Fixed-Price mode.

HUD's Move to Modernized Systems and Processes

Mission Process 1 – Helped HUD design and implement a roadmap for change

Mission Process 2 – Reengineered HUD's server environment

Mission Process 3 – Helped HUD establish a large-scale Government private cloud

Results:

- HUD raised its Federal Information Security Management Act (FISMA) rating from F to A+ within two years of the start of the HITS contract.
- HUD achieved a coveted milestone—a "green" rating on the Policy Management Authority (PMA).
- HUD now has a very agile, responsive, highly available, scalable IT environment that runs its legacy applications and allows HUD's next-generation web applications to go live on time and successfully.

Our fixed-price M&O Resource Unit includes preventive maintenance, application updates and patches that do not involve new functionality or enhancements, continuous monitoring and fine-tuning for optimal performance, and, of course, all activities required to achieve restoration of service (i.e., break/fix). HPES will develop process improvements and automation to reduce the cost of the M&O services. All application patches for routine maintenance and/or restoration of services will include UAT.

2.10.10.2. Process used to migrate developed Applications into (and retire/decommission Applications from) the Applications Portfolio, including the approach, data requirements, timeframes, and analytic approaches to ensure a reasonable fixed price for Applications M&O Services.

Throughout the year, applications are added and retired from the Applications Portfolio. The County initiates additions and retirements as an approved request.

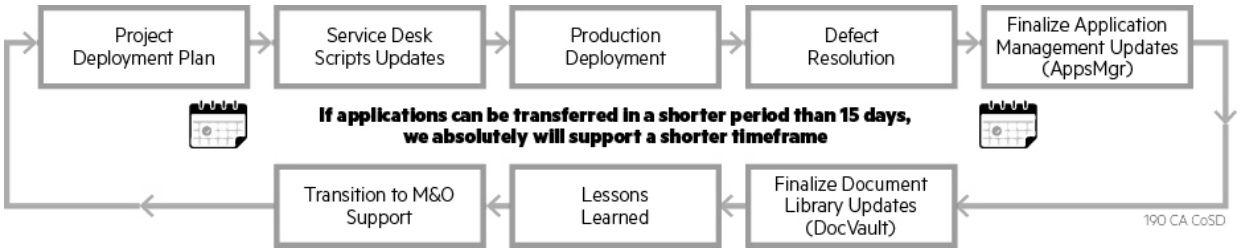
When adding an application to the M&O portfolio, unless modified by a Service Request, Portfolio Applications shall be added into the appropriate FFP M&O bundle immediately upon implementation into production or the expiration of a stated warranty period, whichever is later. Addition includes updated Service Desk scripts and entry of application details into the AppsManager tool. Support for the application will now be part of the M&O firm fixed price (FFP).

For addition of a large, complex such as Connect Well San Diego or implementation of an additional module to an existing app, such as adding Open Enrolment to PeopleSoft, a service request shall be delivered to Contractor to perform M&O activities for up to 6 months.

Large, Complex is defined as a Portfolio Application modification estimated at 1500 or more total labor hours.

During this time Contractor will gather and report M&O support 'actuals' to determine the future adjustment to the appropriate FFP Bundle.

Figure 141. Post Production Care Plan



Conversely, if an application is to be removed (retired) from the M&O portfolio, the M&O team will perform all functions required to retire that application, including decommissioning the infrastructure and updating Service Desk scripts. Applications are/will be retired by the direction of the County using a non-billable work order request. Retiring an application typically results from the addition of a new application or procedure that deems the current application obsolete.

On a quarterly basis, the Application Review Board, with participants determined by County CIO and Contractor AE, shall review all impacted billing low-orgs to determine if growth or reduction adjustments are required to either one or more Applications FFP bundles or the FFP Dev/Test RU.

Material changes are additions or deletions of Portfolio Applications that effect the M&O support or server environment. Material is defined as adding or deleting a Portfolio Application with one or more of the following:

* Fifty (50) or more End-Users
* Adding or deleting five (5) or more servers to Dev/Test
* Adding or removing an app representing >30% of a billing low-org

As described in Section 2.10.1, all changes will be evaluated by the Applications Review Board and go forward recommendations will be made.

HPES will develop process improvements and automation to reduce the cost of the M&O services.

2.10.11. Your proposed approach for ensuring that Third-Party Software packages are updated to current versions. Describe the frequency with which your organization typically implements upgrades. Describe the process your organization undertakes from initial testing through production implementation and the value added by this process. Describe the process which will be followed to keep County representatives aware of the availability of Third-Party Software package upgrades.

Approach. HPES will catalog and track all third-party software used by the County to make certain that software is maintained to the current versions. HPES will report to the County application primary contact on third-party software with upcoming updates. Through an approved request for change (RFC) and change control process, we will meet with the County and will recommend third-party software upgrades. All changes will follow Change Control Review Board (CCRB) in accordance with County processes and procedures for third-party software.

Frequency. HPES will proactively track upcoming updates to third-party software through the Internet, direct contact of third parties, and/or by announced vendor notices or technical updates. Upgrade frequency to third-party software will depend on the software vendor and County direction.

As new patches from third-party vendors are received. HPES will determine along with the County, if the release includes enhancements or new functionality. HPES will make maintenance change (including restoration of service or maintenance patches/upgrades) to production applications upon a County-approved request for change (RFC). Upgrades to an application that will provide new features and/or

functionality will be supported under application development services via a Service Request. HPES will meet weekly with the County to review the pool of RFCs and determine the priority and whether it should be approved for implementation. HPES will schedule the implementation of approved RFCs based on County priorities

Upon approval of the County CCRB, we will initiate the process for upgrading third-party software as outlined below.

Currently, weekly meetings are held between HPES and the County CCRB in which decisions on upgrades are addressed. If greater frequency is required, HPES may request on a case-by-case basis an emergency meeting of the County CCRB specific to any urgent upgrades that HPES believes require immediate County attention and approval (for example, patches that remediate security vulnerabilities).

Process — Testing Through Implementation. Once HPES receives an upgrade, we will stage that upgrade in our lab and run tests in accordance with our Standard Procedures.

Initial testing will start with the development of a testing plan and installation of the patch release/upgrade in a Dev/Test environment. Staff from HPES and the County will test the new version of the third-party software.

User acceptance testing (UAT) may include specific testing scripts and scenarios, depending on the application and the amount of enhancement. Once UAT is completed, results will be presented to the County for approval and signoff.

Upon UAT approval, HPES will schedule and prepare for software installation into the production environment. This process is consistent with existing County processes and lends itself to a predictable, reliable, and controlled approach for upgrading third-party software for the County.

Upgrade Availability Communication. HPES meets weekly with the CCRB to review the recommended changes. Together with the County, we will discuss and evaluate the change for consideration. Each proposed change must be approved by the County CCRB and the County representative. At such time that the proposed change is approved, we will schedule the change to accommodate the application downtime window.

Applications Services Framework – Executive Summary

Our Applications Services Framework solution will demonstrate benefits to County employees, taxpayers, and residents. We will continue to provide application innovations enabled on multiple platforms and dedicate our team to meeting the County's key IT initiatives.

The County's exchange of ideas with our applications team has created an exciting environment for our personnel supporting the County. Whether sustaining applications in our M&O services or helping to create new applications, our HPES Applications Services team has a strong commitment to meeting the future needs of the County. In Table 63, we list the features of HPES Applications Services and their benefits to the County.

Table 63. Features of HPES' Applications Services and their Benefits to the County

FEATURES OF HPES APPLICATION SERVICES	BENEFITS TO THE COUNTY
Experienced Application M&O Manager, Tina Terlecki, and Application Development Manager, Mark Roehr	Create collaborative applications services environment and County confidence that applications will remain reliable while innovative development is pursued

All M&O applications transition to the Fixed-Price Model	Provides predictable costing for all M&O applications with a goal of reducing overall costs
Applications Development Waterfall, Iterative and Agile Methodologies	Provides on-time deployment of applications that meet key IT initiatives of the County's IT Strategy
HPES team capability in application deployment for use on multiple platforms (e.g., desktop, tablets, iPad, mobile phones)	Enables users requiring County services to take their mobile devices to the beach and check water quality and traffic alerts as well as obtain emergency services
A applications services team that lives in and knows the County and how it does business	Fosters citizen-centric applications development and community feeling among residents

2.11 Transition Services

Exhibit D, Schedule 2.1

Executive Overview

As the incumbent, HPES offers the County the lowest-risk transition. As we are not learning a new environment or making major delivery changes during transition, HPES is not encumbered by the extensive transition activities such as job shadowing and knowledge transfer. We can give the necessary attention and focus to the Transition projects, adding value while continuing to support the current environment. We will use our well-defined and industry-leading Transition and Transformation Methodology (TTM), established County relationships, and understanding of the needs related to overall transition and the six defined Transition Projects that will support the continued growth and maturation of the County of San Diego. Our transition plans have the features and benefits shown in Table 64.

Table 64. Transition Plans Features and Benefits

FEATURES	BENEFITS
• Well-known HPES leadership team with existing relationships • Transition leadership and expertise, County experience, and large-program operations experience • TPMO and proposed governance structure to address issues and risks promptly via daily briefings - transparency with County • TTM methodology proven at the County and on other major programs • Supplemental expert staffing to support Transition Projects	• Lowest risk • Least complexity • Value-add on each project • Clear identification of transition activities and consolidated plan • Improved service and customer satisfaction

HPES brings the lowest-risk transition.

We will use our TTM as the basis for managing overall transition as well as the transition projects. TTM provides a comprehensive yet flexible, ITIL-aligned framework so that every aspect of the transition is accounted for, planned for, and expertly managed. TTM addresses the people, business processes, and technology issues of transition and provides a step-by-step process for joint planning, communication, and management. The Transition Program Management Office (TPMO) will have primary responsibility for planning and executing the Transition Plan. We will define and identify key linkage points in the County of San Diego organization. We assigned a senior and experienced Transition Program Manager (TPM), Chris Spanka, who will direct and lead all aspects of the Transition and will work collaboratively and transparently with the County and our existing Program Management Office (PMO). The TPM will

facilitate daily stand-up calls and issue weekly status reports to provide transparency and make sure that key decision-makers and the County stakeholders are fully aware of progress as the transition program proceeds.

Chris will lead a clearly defined TPMO, with full accountability for execution. He will report directly to our Account Executive, Cathy Varner. In partnership, they will execute on-going operations and the transition projects. Important factors in the transition that help facilitate highest service and quality are the transition schedule, timely staffing, and clear and concise communication.

Requirements (Schedule 2.1, Section 2)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary

As the incumbent service provider, HPES is able to move directly into execution of the County's transition projects immediately upon Contract Effective Date (CED). We will not need to perform any of the tasks in the sections listed in Table 65.

Table 65. Transition Tasks

REQUIREMENTS SECTION	TRANSITION TASK	BENEFIT TO THE COUNTY
2.1	Human Resources Transition	With no Human Resources activities taking place, staff are fully focused on County service and project delivery
2.2	Knowledge Transfer	Our staff can continue to provide seamless support during the transition
2.3	Asset Transfer	All assets and leases remain intact
2.4	Assignment or Management of Third Party Contracts/ Licenses/ Leases	All contractual relationships remain intact
2.5	Data Transfer	All data remains intact and secure. Only data residing in Plano will need to be migrated.
2.6	Compliance with Service Levels	HPES will continue our strong record of high service level performance from the first day of the contract
2.7	Assumption of Current Projects	All current projects will continue with no delays. As part of our transition planning process, we will blend these project schedules with the transition project schedules to make sure that all County project deadlines and budgets are met, and any potential conflicts in scheduling of activities are resolved according to the County's priorities

Our solution summary for the remaining requirements follows.

2.8 Communications/Governance Plan for the County and the Legacy Provider

We will provide a Communications and Governance Plan as part of the Transition Initiation activities, so that all communications are clear and any issues are managed to rapid resolution.

2.9 Contingency Planning/Risk Mitigation

Our Transition and Transformation Methodology (TTM), described below, includes a robust process for Risk Management that will make sure risks are mitigated to the County's satisfaction.

2.10 Measurable Success Criteria

Each project will, at its inception, include a step where HPES and the County mutually agree on the definition and measurement of success. This will provide a smooth cutover process as each framework and project is completed. Success criteria are of two types:

- Project management success criteria:
  - Signoff of tasks and deliverables according to the dates in the project plan. This will be measured and reported weekly according to task completion.
- Project deliverable success criteria:
  - Verification that the business objectives set out for the project were met.

The Transition Services Manager will be responsible for working with the County to define the overall success criteria for the program, and each Transition Project Manager will be responsible for managing to and measuring the success criteria for each project under his/her purview—these also roll up to the overall program level. Measurements and tracking against defined criteria for each project will be reported to the joint Transition Management Office (TMO) weekly. Any measurements that indicate that one or more success criteria are in jeopardy will be escalated to leadership for determination of how to remediate or prevent further issues.

Measurement of success criteria may be discrete (pass/fail: either the criterion was met or it was not) or continuous (measurable on a scale, such as a range of percentages). Since project deliverable success criteria will be relevant to the County, following are some examples of project deliverable success criteria suggested for this program, along with their measurement approach. This is not intended to be an exhaustive list: as previously noted, actual success criteria will be established for each aspect of the Transition.

PROJECT	DEFINITION OF SUCCESS	MEASUREMENT APPROACH
Overall Transition Program	Sustainment or improvement in customer satisfaction	• Service Level Measurement, before, during, and after the Transition • Periodic customer surveys, specific to the Transition experience and effectiveness of communications
Disaster Recovery Plan	Completion of one table-top or actual failure exercise according to the new plan	Record levels of participation, scope, and end results and remediation recommendations
Data Center Consolidation	Sustainment or improvement in application performance	Verification by stakeholders that an application migrated to the consolidated data center environment performs as well as

PROJECT	DEFINITION OF SUCCESS	MEASUREMENT APPROACH
		or better than it did in its previous environment (as measured by batch job execution times or transaction response times) measurements will be taken and compared against established baselines conducted and documented prior to Transition, using existing tools such as Autosys or Load Runner or using system based monitors such as performance manager
Email Migration	95% of mailboxes migrated in the first pass without subsequent issues, post-pilot; all remaining issues resolved within 24 hours.	Project team migration results report
Storage Architecture	Zero data loss	Verification from migration tools of successful completion
Development/Test Environment	Successfully implemented Broker and Managed Private Cloud, with all assets assigned to the correct pools	Audit of assets before and after project to verify assignment
Service Portal	80% of End-Users trained on Portal features	Measurement of End-User participation in training

2.11 Transition Project Plan

As part of developing this proposal, we created an initial high-level project plan. In the sections that follow, we use segments of that plan to describe the high-level steps we will follow in executing the transition management and project execution. During Transition Initiation, we will work with the County to develop the lower-level details of that plan. Our in-depth knowledge of the environment and the County business enables us to develop and execute the plan in an iterative fashion. We can adapt the plan quickly in response to changing needs.

The plan information for each framework can be found as follows:

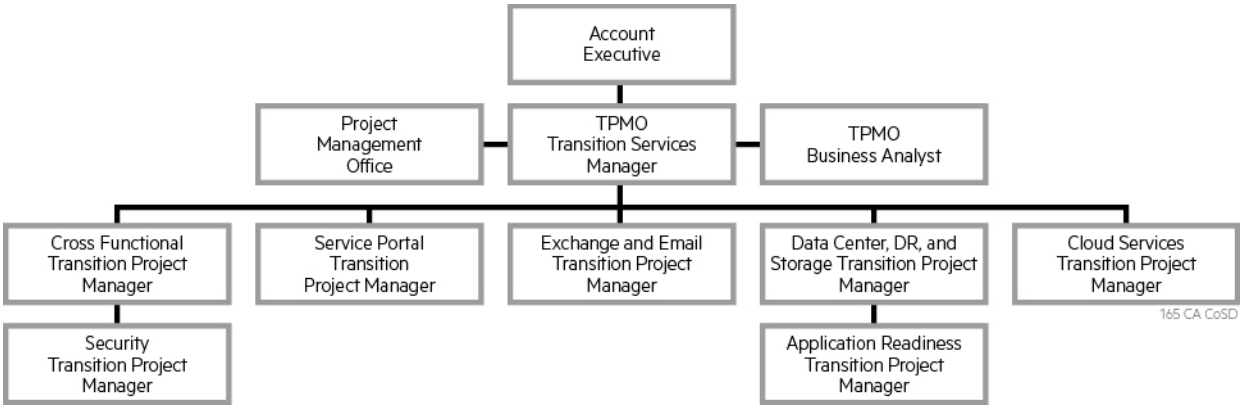
FRAMEWORK	TRANSITION PLAN
Service Desk	• Cross Functional Transition Schedule and Tasks, Page 506 • Response to Section 3.6, Page 511
Application Services	• Cross Functional Transition Schedule and Tasks, Page 506 • Special Cross Functional Projects – Application Services Framework, page 511
End User Services	• Cross Functional Transition Schedule and Tasks, Page 506
Network Services	• Cross Functional Transition Schedule and Tasks, Page 506

FRAMEWORK	TRANSITION PLAN
Data Center Services	• Cross Functional Transition Schedule and Tasks, Page 506 • Special Cross Functional Projects – Data Center Services Framework, Page 515 • E-Mail Services – Response to Section 3.2, Page 519 • Development and Test Environment – Response to Section 3.3, Page 527 • Consolidated and Single Data Center – Response to Section 3.4, Page 533 • Storage Architecture – Response to Section 3.5, Page 562
Cross Functional Services	• Cross Functional Framework Transition: Activities Aligned to Framework Components, Page 515 • Special Cross Functional Projects – Other, Page 515

2.12 Transition Staffing (Transition Management Specific Question 2.11.1.4)

A critical component of our TTM is creating a Transition Management Office (TMO). This approach engages all key stakeholders, implements a structure that fosters collaboration, and makes stakeholders accountable for a successful transition. Figure 142 shows the TMO structure and the roles, functions, and key responsibilities of each member.

Figure 142. Transition Management Office



Dedicated Transition Project Managers will drive each project's success while managing to the integrated plan.

The goal of the TMO will be to create and refine joint program schedules, manage risks, resolve issues, provide proper communication, assess progress, and facilitate on-time transition completion. The TMO will serve as a central conduit for information, communication, and cooperation. In addition, the TMO will manage all project reporting and quality assurance activities to verify that HPES follows all established Project Management standards and that project reporting is consistent.

Additional details on roles and responsibilities for the identified TMO staff are presented in the following table. Each Transition Project Manager will be responsible for the following items:

- Establishing and documenting progress on their individual sub-project plan(s) within the overall master schedule, and coordinating interdependencies with other projects
- Managing the activities of the technical teams working on their projects, in coordination with the current HPES support staff and within the established operational delivery processes
- Reporting project status to the TMO with the Project and Portfolio Management (PPM) tool

- Managing issues and mitigating risks that arise, with escalation when appropriate
- Making sure that their project team meets established success criteria and facilitating handoff of the project's deliverables to operations leadership
- Performing close-down of the program.

The role of each TMO team member is briefly described in Table 66.

Table 66. TMO Roles and Responsibilities

TMO ROLES	TRANSITION RESPONSIBILITIES
Transition Services Manager	The Transition Services Manager oversees the Transition results, deliverables, schedules, and dependency tracking across all Transition projects. He is responsible for all Transition activities, including Transition kickoff sessions, program and project management, risk management, communication, reporting, Transition escalations, change management, quality management, operational readiness reviews, and coordination with any in-flight projects. The Transition Services Manager performs quality checks during Transition, working with the HPES account team to make certain that the team conducts all activities in accordance with established practices. Christopher Spanka, a seasoned Senior Program Manager with more than 34 years of experience in IT—and previously engaged in the Account tools analysis and health check—will serve in this role.
Service Portal Transition Project Manager	Responsible for the project to implement and customize the Service Portal, within the Service Desk Framework (Schedule 2.1, Section 3.6).
Data Center Consolidation Project Manager	Responsible for the Data Center Consolidation Transition project within the Data Center Framework. This will include the following projects: • Buildout and migration to the new Data Center Network compartment in Tulsa, and establishment of connectivity to the disaster recovery (DR) site (HPES-defined sub-project). • Buildout of the new Storage Architecture (Schedule 2.1, Section 3.5). • Establishment of the new DR infrastructure to support subscription services in the Colorado Springs HPE Continuity Center. • Execution of the consolidation of all County Data Center workloads currently residing in Plano into the Tulsa Data Center (Schedule 2.1, Section 3.4).
Cloud Services Transition Project Manager	Responsible for setting up and configuring the Managed Private Cloud (MPC) and the Helion Managed Cloud Broker (HMCB) in the Tulsa Data Center and configuring the Development and Test Environment (Schedule 2.1, Section 3.3) within the Data Center Framework.
Application Readiness Transition Project Manager	Works with the Data Center Consolidation Transition Project Manager to coordinate application
Exchange/Email Transition Project Manager	Responsible for migrating the County to the Office 365 email solution within the Data Center Transition Framework (Schedule 2.1, Section 3.2).
Cross Functional Project Manager	Responsible for the following projects within the Cross-Functional Framework:

TMO ROLES	TRANSITION RESPONSIBILITIES
	• Oversight of the delivery of new Standards and Procedures, Service Level Management and Reporting artifacts (or updating current versions to meet the new contract requirements) for all Cross-Functional Framework Components, as well as for the other Frameworks • Management of development and implementation of the Cross-Functional Framework Component Management Plans • Coordination of delivery of Disaster Recovery Plans for each Framework.
Security Transition Project Manager	As part of the Cross-Functional Framework, the Security TPM is responsible for coordinating execution of Security and Identity Management related projects and changes within the other Frameworks.
TMO Business Analyst	Responsible for administrative support, such as coordinating status reports and meetings, project schedule change management and integration, and quality management on project deliverables.

Our Transition Management Office will be staffed and ready to begin. The technical teams who will deliver the transition projects are identified.

During the Transition period, we will augment our technical staff with additional resources to make sure the Transition projects execute successfully, without creating undue constraints on the current support teams. Where appropriate, we may temporarily backfill select members of the local team supporting the County so that they may lend their expertise and County knowledge to the implementation of some Transition projects. We will make sure, however, that this does not cause any disruption to the County's current services and projects. In this way, these team members gain hands-on experience with the new tools and technologies and carry that experience forward in support of the County post-Transition.

2.13 Transition Schedule

Because we can start immediately on the Transition projects—without having to address staffing, knowledge and asset transfer, and other turnover matters—we provide greater assurance that we can meet the County's schedule as defined, without impacting other activities, even with the high degree of interdependencies among the projects.

Rationale

HPES' transition solution provides the County with a seamless, minimal risk transition. With the transition projects' significant interdependencies, we will make sure that we manage at the program level—to coordinate and track all of the sub-projects. We will also manage each significant sub-project as a project, while continuing to provide excellent service delivery under our current contract with the County. During the Transition period, we will build on our more than 10 years of County relationships to successfully plan, communicate, and manage the transition activities collaboratively. We have a detailed understanding of how to configure the County's applications and environment to meet the business needs. Our plan during the Transition period is to have in place the right people from HPES, AT&T, and the County, who understand all the moving parts of these changes.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Resources. As noted above, we will provide dedicated resources for Transition project management and execution to make sure that operational delivery and the County's current projects are not impacted by resource constraints.

Facility. The HPES Transition teams will support the Transition from our Rancho Bernardo office and existing County locations, where appropriate, as well as HPES facilities in Tulsa, OK, and Colorado Springs, CO. TMO resources, including the Transition Services Manager, will operate out of Rancho Bernardo.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

HPES will execute project management, transition, and transformation by using our Transition and Transformation Methodology (TTM) composed of standardized processes, methods, tools, and governance to deliver repeatable and predictable results. It addresses the people, business processes, and technology issues of transition and provides a step-by-step process for joint planning, communication, post-contract verification, and management.

HPES TTM Process

To achieve our goals and reduce risks, costs, and complexity of transition, HPES will use our comprehensive and proven TTM, a flexible comprehensive framework of robust processes, procedures, best practices and supporting assets that enable the successful planning and execution of a Transition or Transformation program. It defines what deliverables are to be produced, what work needs to be done, who should do it, how they should do it, and when it needs to be done. It also provides supporting assets to complete the work efficiently. We have refined TTM in practice with Government agencies and commercial organizations of all types and sizes since 1998, using it successfully on more than 1,000 transitions.

Transition programs and their associated projects will go through five distinct phases: Initiate, Plan, Execute, Monitor and Control, and Close.

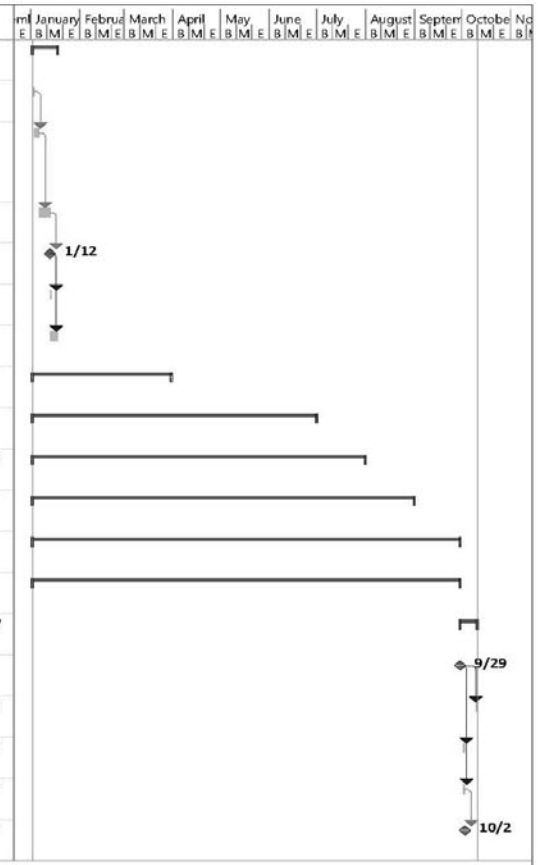
Initiate. HPES and the County will set up the program management structure described above, onboard the program team, and start the program. During the first few days of the Transition, our TMO will create draft versions of the Communication Plan, Governance Plan, and the initial master Transition Project Plan and Schedule. We will start from our template repository and work with the County collaboratively on these items, but will also submit a final draft for formal County approval as required. Once finalized and approved, we will put these plans into action and begin program execution.

Plan. Building on the notional Transition Plan developed during the proposal process, we will conduct detailed joint planning to elaborate and refine the plan, then conduct a transition kickoff meeting with identified key stakeholders from the County, the current delivery leadership—as represented by our key personnel—and key leaders from the Transition Technical teams.

The TMO will create a master Transition Management Plan along with a corresponding Transition Schedule. This will serve as the overall foundation for the program and will address the key program elements, including resources, dependencies, and timeframes. This master plan and schedule will be augmented for each of the six Transition projects. Figure 143 provides a high-level timeline of Transition activities, showing the Transition Initiation, the Framework Transitions, and the Final Transition Milestones (as defined by Schedule 2.1, Section 4) that follow at the end of the Transition period. All timeline figures have been updated for the Final response.

Figure 143. Transition Timeline Showing Initiation and Final Milestones

ID	WBS	Task Name	Duration	Start	Finish
1	1	**Transition Initiation**	**12 days**	**Mon 1/2/17**	**Tue 1/17/17**
2	1.1	Assemble Transition Management and Technical Teams	1 day	Mon 1/2/17	Mon 1/2/17
3	1.2	Develop Communications and Governance Plan, draft Project Plan and Schedule (initial program deliverables)	3 days	Tue 1/3/17	Thu 1/5/17
4	1.3	County reviews submitted deliverables	5 days	Fri 1/6/17	Thu 1/12/17
5	1.4	County response or approval received	0 days	Thu 1/12/17	Thu 1/12/17
6	1.5	Finalize and Implement Communications and Governance Plan	1 day	Fri 1/13/17	Fri 1/13/17
7	1.6	Conduct Kick-off Meetings	3 days	Fri 1/13/17	Tue 1/17/17
8	2	**Service Desk Framework**	**64 days**	**Mon 1/2/17**	**Thu 3/30/17**
65	3	**Application Services Framework**	**130 days**	**Mon 1/2/17**	**Fri 6/30/17**
121	4	**End User Services Framework**	**151 days**	**Mon 1/2/17**	**Mon 7/31/17**
161	5	**Network Services Framework**	**174 days**	**Mon 1/2/17**	**Thu 8/31/17**
201	6	**Data Center Services Framework**	**195 days**	**Mon 1/2/17**	**Fri 9/29/17**
397	7	**Cross Functional Framework**	**195 days**	**Mon 1/2/17**	**Fri 9/29/17**
444	8	**Final Transition Milestones**	**7 days**	**Fri 9/29/17**	**Tue 10/10/17**
445	8.1	All Service Levels cut over	0 days	Fri 9/29/17	Fri 9/29/17
446	8.2	Deliver first invoice covering all Services (Draft Invoice)	1 day	Tue 10/10/17	Tue 10/10/17
447	8.3	Provide listing of HPES Personnel to reside at County Locations	1 day	Mon 10/2/17	Mon 10/2/17
448	8.4	Provide Key Personnel update	1 day	Mon 10/2/17	Mon 10/2/17
449	8.5	All Transition activities complete	0 days	Mon 10/2/17	Mon 10/2/17



Page 1

Note that the notional schedule used throughout this section uses a start date of 1/2/2017 for the CED. We recognize that the CED will be established by the County after award, and the actual transition dates will change accordingly. In the sections that follow, the high-level steps of the Transition project are expanded on and described.

Execute. Within the TTM methodology, each Transition Project Plan is executed as described in the sections that follow.

Monitor and Control. Throughout the program, the TMO will oversee the Transition activities to produce deliverables on time, remain within budget, and execute Change Management if needed.

Close (Final Transition Milestones). We will mutually verify that commitments and success criteria defined in the Transition Management Plan have been met and formally accept the completion of the implementation projects and program. We will provide an updated key personnel listing, if necessary, and list HPES personnel to reside at County locations. The Account Executive and the Billing Management Services staff will be responsible for delivering the first invoice covering all services.

- Automated Tools – Automated systems and tools involved in proposed solution

Table 67 lists the tools we will use to support the Transition program. TTM has a large body of templates and artifacts that we have used on successful transitions with scopes similar to this one. A few of these are described below.

Table 67. Tools Utilized to Support Transition

TOOL NAME AND VENDOR	DESCRIPTION
TTM Templates	• Integrated Transition and Transformation Plan (ITTP) • Transition Specific Risk Register (Excel) • Communication Plan (Word) • Governance Plan (Word) • Transition Daily, Weekly Meeting minutes (Word) • Operational Readiness Checklist / Success Criteria (Word)
Project-specific Tools	• HPES will use Microsoft Project to coordinate and manage Transition-related projects and tasks. • Tools used for Transition projects will be defined and covered in the related sections.

- Qualifications and Experience – Background and experience in comparable environments

Regarding specific program experience, in addition to our experience supporting the County, we can draw on major infrastructure support experience from across HPES. Table 68 provides highlights.

Table 68. Highlights of What We Do to Support the County

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND RELEVANCE TO THE COUNTY
County of San Diego	• We transitioned successfully from Northrop Grumman (NG) in 90 days in 2011, when HPES took over as prime contractor. • Many of the leadership and support teams who made that transition are still on the account.

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND RELEVANCE TO THE COUNTY
Centers for Medicare & Medicaid Services Enterprise Data Center (CMS EDC)	We transitioned workloads from six different CMS data centers into our data center. Our transition team developed the transition plans and led the transition activities. The team managed and supported all activities associated with the workload transitions. • We worked closely with all CMS business owners and the incumbent application hosting services provider to schedule migrations during times and in a manner acceptable to the legacy production data centers. • We worked closely with CMS' business application governance teams. • We deployed start-up teams of experienced specialists, including design engineering; system administration; network engineering; security, backup, and restore; and storage and monitoring experts. To reduce risk, we used proven, repeatable processes and refined them from transition to transition. We used our TTM on this transition.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

2.11.1 Transition Management Specific Questions (2.11.1.1 - 2.11.1.5)

Answers to Specific Questions – Listed below are questions relating to topics of particular interest – if answers are provided already in the context of responses to these Service Framework Components, note in your response with specific cross-references to the questions.

2.11.1.1. Describe your proposed approach for transitioning licenses, contracts and leases from the Legacy Provider and the County

As the Legacy Provider, HPES will not have to transition licenses, contracts, or leases. We will continue to use our existing processes to support and manage all third-party vendor relationships, licenses, contracts, and leases. These processes are described in Section 2.5 of the Technical Proposal.

2.11.1.2. Describe in detail your proposed approach for transitioning Portfolio Applications from the Legacy Provider. Include potential impacts to schedule and technical hurdles.

As the Legacy Provider, HPES will not have to transition portfolio applications. The data center consolidation project schedule will be built to consider and avoid any impacts to current application projects whenever possible.

2.11.1.3. Describe your proposed approach for transitioning management responsibility for work in progress from the Legacy Provider

As the Legacy Provider, HPES will not need to transition management responsibility for work in progress.

2.11.1.4. Describe your approach to using Transition resources who will remain to provide Operational Services for the County versus resources who will transfer after Transition?

HPES' staffing approach/strategy is to provide dedicated resources for each transition project. We will leverage current HPES resources supporting the County to assist, as described above in the Requirements Section on Transition Staffing (response to Schedule 2.1, Section 2), and our staffing plan includes subject matter experts (SME) to augment and make sure that there are no impacts to operations activities.

2.11.1.5. Do you have any alternative approaches to Transition Plan or sequence for County consideration?

HPES uses TTM and has standardized this methodology to successfully manage and deliver on more than 1,000 transitions during the past 46+ years. We have aligned our Transition Plan with the County's timeline, and are not proposing any alternative sequencing or approaches at this time. We will review and refine this plan with the County after award to gain County approval.

Cross Functional Services (Schedule 2.1, Section 3.1)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary

HPES' plan for the Cross Functional Services Transition is to focus on the Process, Service Level Management, and Reporting changes needed for each of the technical frameworks (Service Desk, Applications, Network, and Data Center) to meet the County's requirements for the new Contract. This same focus will apply to the Cross Functional Framework itself—at the component level. In addition to these three focus areas, we will implement Security and Identity Management changes required to meet each framework's new delivery model, in those cases where changes are required. The cross functional activities for each framework will be implemented in parallel but in coordination with that Framework's Transition projects, where applicable. For frameworks that do not have specific transition projects identified, the Cross Functional Transition will be the only scope of that framework's transition; therefore, all Framework Transition activities outside of the specified Transition projects are described in this section.

The new Cross Functional components, as defined in the solicitation, represent services that we provide today, and we appreciate that the County has recognized their value by defining them as requirements for the new Contract. We agree that by solidifying and focusing on capabilities such as Business Analysis, Service Delivery Management, and the ITIL disciplines of Incident, Problem, Change, and Release Management, the County's IT Service Frameworks supported by these functions will improve even further in quality and customer care. To that end, during the Transition period, we will develop a management plan for each of the Cross Functional component areas—both existing and newly formalized—and train our teams on the changes. Each of the Cross Functional components will also have some degree of Process, Service Level Management, and Reporting changes to implement during the 270 days of the Transition period, so these efforts will follow a similar approach to that of the other frameworks.

Rationale

HPES' overarching approach is to improve existing processes or to establish the new ones based on methods that have proven successful in the County of San Diego environment. By creating a repeatable set of tasks to be executed across all frameworks and Cross Functional components, the Transition will be more efficient and deliverables will be of higher, more consistent quality than having each framework

address Cross Functional items separately. With each iteration, our Transition Project team will seek to identify improvements to the cycle that will further benefit subsequent iterations. Our primary rationale for this approach is to minimize transition cost, maximize speed to implement improvements, and facilitate ongoing operational stability.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The Cross Functional Transition activities will require input and participation from the current support staff to make certain that new processes and deliverables leverage artifacts and methods currently in place. The Cross Functional Transition team will be embedded with each Framework Transition team.

We will support the Cross Functional Transition primarily from our Rancho Bernardo facility.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

Transition Schedule and Tasks

The chart below is a high-level example of the Cross Functional activities within a Service Framework: End User Services. The same task structure will apply to each framework as well as each Cross Functional component.

In the course of developing this proposal, HPES analyzed the differences between the current and new Contract requirements, and identified the projects needed to prepare our staff for the launch of new initiatives or processes, refresh our documentation or create new deliverables, and gather the metrics needed to measure and improve our services. This analysis will form the basis for creating the detailed plan for execution. Therefore, while the task structure will be the same across frameworks, task durations will vary based on the degree of change being introduced by the new Contract requirements.

The task schedules presented in this section are notional, and we have kept them simple intentionally for illustrative purposes. Although many activities will happen in parallel, once we create the schedule for all Cross Functional components and the Cross Functional activities for each framework, the timeline will expand with the details and dependencies. For example, we will develop new process documentation as the new processes are implemented; as we schedule those activities, the dependencies will modify the timeline from what is shown here.

Figure 144. shows the core high-level tasks we will perform for each framework.

In general, all Cross Functional activities can occur in parallel; however, the degree to which this is true will vary somewhat between the frameworks. For example, a change to a Service Level to meet a higher target performance may require changes to one or more delivery processes to be able to meet it. For some activities, there will be dependencies on other projects taking place in the framework. For example, in the Data Center Framework, the ability to generate new reports and service level metrics from the MPC will be dependent upon completion of that infrastructure's build phase. Because all Cross Functional deliverables are required to be posted to the Service Portal, there is a dependency on the Service Portal's deployment to enable delivery of documents to it.

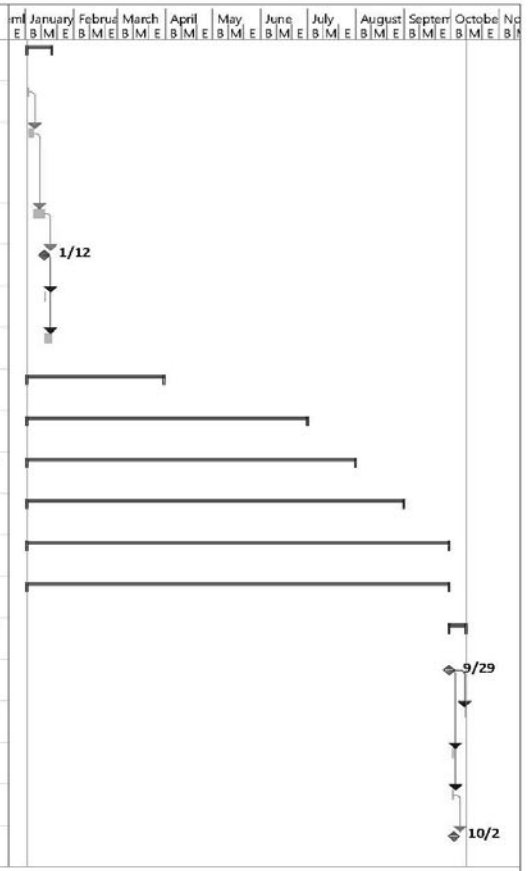
There are no dependencies identified for generation of the Cross Functional Component Management Plans. They will be developed in parallel with, and as the culmination of, the other component artifacts.

Cross Functional Activities Aligned to Service Frameworks

Within each Service Framework, we will follow the basic task structure illustrated in Figure 144.

Figure 144. Cross Functional Transition Activities – Example showing End User Framework

ID	WBS	Task Name	Duration	Start	Finish
1	1	**Transition Initiation**	**12 days**	**Mon 1/2/17**	**Tue 1/17/17**
2	1.1	Assemble Transition Management and Technical Teams	1 day	Mon 1/2/17	Mon 1/2/17
3	1.2	Develop Communications and Governance Plan, draft Project Plan and Schedule (initial program deliverables)	3 days	Tue 1/3/17	Thu 1/5/17
4	1.3	County reviews submitted deliverables	5 days	Fri 1/6/17	Thu 1/12/17
5	1.4	County response or approval received	0 days	Thu 1/12/17	Thu 1/12/17
6	1.5	Finalize and Implement Communications and Governance Plan	1 day	Fri 1/13/17	Fri 1/13/17
7	1.6	Conduct Kick-off Meetings	3 days	Fri 1/13/17	Tue 1/17/17
8	2	**Service Desk Framework**	**64 days**	**Mon 1/2/17**	**Thu 3/30/17**
65	3	**Application Services Framework**	**130 days**	**Mon 1/2/17**	**Fri 6/30/17**
121	4	**End User Services Framework**	**151 days**	**Mon 1/2/17**	**Mon 7/31/17**
161	5	**Network Services Framework**	**174 days**	**Mon 1/2/17**	**Thu 8/31/17**
201	6	**Data Center Services Framework**	**195 days**	**Mon 1/2/17**	**Fri 9/29/17**
397	7	**Cross Functional Framework**	**195 days**	**Mon 1/2/17**	**Fri 9/29/17**
444	8	**Final Transition Milestones**	**7 days**	**Fri 9/29/17**	**Tue 10/10/17**
445	8.1	All Service Levels cut over	0 days	Fri 9/29/17	Fri 9/29/17
446	8.2	Deliver first invoice covering all Services (Draft Invoice)	1 day	Tue 10/10/17	Tue 10/10/17
447	8.3	Provide listing of HPES Personnel to reside at County Locations	1 day	Mon 10/2/17	Mon 10/2/17
448	8.4	Provide Key Personnel update	1 day	Mon 10/2/17	Mon 10/2/17
449	8.5	All Transition activities complete	0 days	Mon 10/2/17	Mon 10/2/17



Page 1

Standards and Procedures. We begin by inventorying and reviewing each procedure document against the new Contract requirements to identify the subset of processes that need to be changed or created (if a new process is needed). We then categorize the documents based on the degree of changed required:

- Completely new procedure or standard needed – If a new process is being implemented in support of a new technology, our Solution Guide documentation for the service offering that we are implementing will provide a base set of procedure documents. From there, we will customize and adapt those base documents to the specifics of the County's environment and documentation standards. We then test the procedure and further refine the documentation. If a new procedure is needed based on a new business requirement, we can use our Enabling Delivery and Global Excellence (EDGE) repository to locate a base artifact from which to build the new procedure.
- Updates required to an existing procedure – We follow a similar process to the one for a new procedure/standard, but the starting document is the existing process. Whether testing is required will depend on the degree of change.
- Existing procedure continues unchanged – No modifications required.

Once the Standards and Procedures drafts are complete, we will submit each draft to the County for review and response. The County will reply within the agreed timeframe if any changes or clarifications are required. We will then make the final set of modifications, if needed, and finalize the documentation. Documents will be posted to the appropriate repository reachable from the Service Portal. Any procedures or standards that are no longer valid will be retired and their documentation archived according to our Records Management policy.

Where appropriate, we will provide training in and/or communications about new or modified procedures and standards to our staff and to County stakeholders who participate in or are customers of the process. Training methods will range from Frequently Asked Questions (FAQs) and tip sheets, to training videos accessible from the Service Portal, to webcasts or onsite training at our Rancho Bernardo site.

Service Level Management. There are a number of new and modified Service Levels in the new Contract. During the Cross Functional Transition, we will follow these steps to implement them.

For each new or modified Service Level, we will identify the data necessary to calculate it, the process to verify data quality and scrub exceptions, and any scripting or automation needed to manage the data and its reporting to the Service Level Management process.

We then will develop and test the new or updated metrics collection process, checking the data and the performance metrics.

We will identify the appropriate process or service improvements needed to meet the Service Level and test them for an additional month to determine whether this brings us to an acceptable level of performance. Generally, no more than one to three iterations of baseline measurement and adjustment are required to identify the scope of operational change required by the Service Level. The time to complete this process will be within the time allocated for transition of the applicable framework.

Once we have successfully achieved the new performance target, we will proceed to update all process and reporting artifacts, and present them for County review and response, according to the steps described above in Standards and Procedures. After finalization, we will post all deliverables to the appropriate repository, available from the Service Portal.

Once implemented, our Service Level metrics are integrated into the Service Level Dashboard (currently known as the Minimum Acceptable Service Level [MASL] Dashboard), available from the Service Portal. Any Service Levels no longer required will be removed from the Service Level Management process.

Reports/Deliverables. Transition activities for creating new or modified reports are similar to the tasks defined for updating Standards and Procedures: We begin by inventorying and reviewing each report against the new Contract requirements to identify the subset of reports that need to be changed or created (if a new report or deliverable). We then categorize them based on the degree of changed required:

- New report needed – If a new report is being implemented in support of a new service, our Solution Guide documentation for the Service Offering that we are implementing will often provide a base set of reports. From there, we will customize and adapt those deliverables, or the automated scripts that create them, to the specifics of the County's environment and reporting standards. We will then test the report and further refine the process. If a new deliverable is needed based on a new business requirement, we can use our EDGE repository to locate a base artifact from which to design and automate the new report.
- Updates required to an existing report – We follow a similar process to the above, but the starting point is the existing report process.
- Existing report continues unchanged – No modifications required.

Once drafts of the new or modified reports for the framework are ready, we will submit them to the County for review and response. The County will reply within the agreed timeframe if any changes are required. We will then make the final set of modifications, if needed, and finalize the generation procedures and formats, and place the reports into an automated schedule wherever possible. Process documentation will be posted to the appropriate repository, as described above, and new reports will be added to the standard reporting cycle. Any reports that are no longer valid will be retired and their documentation archived according to our Records Management policy.

Where appropriate, we will provide training in and/or communications about new or modified procedures and standards to our staff and to County stakeholders who participate in or are customers of the process. Training methods will range from FAQs and tip sheets, to training videos accessible from the Service Portal, to webcasts or onsite training in our Rancho Bernardo site. For reporting, the lighter electronic communication formats are generally sufficient.

Security and Identity Management Updates. The new Contract identifies a number of areas where security posture is being heightened, and the projects being implemented in the new frameworks will require some security-related sub-projects. We describe these in the section on the Security Management Component that appears below. In general, the tasks will follow the steps illustrated in the Gantt chart, but for security sub-projects, a good deal more detail will be added to address specific requirements.

Framework Disaster Recovery Plan. For the new Contract, we have added disaster recovery (DR) specialists to augment the team. They will be dedicated to maintaining these plans and overseeing DR testing. They will join the Cross Functional team during transition to lead the DR plan updates for each framework. Each framework will have its DR plan reviewed and updated to support the requirements of the new Contract. The DR plan will be submitted in draft form for County review and comment, then finalized and delivered to a restricted area of the Service Portal no later than 90 days prior to the framework cutover[3].

In the sections that follow, we highlight some of the special sub-projects that will occur in each Framework's Cross Functional Transition.

[3] For the Service Desk Framework, since 90 days prior to cutover is equivalent to the Contract Effective Date (CED), we will deliver the DR plan at CED + 30 days.

Special Cross Functional Projects – Service Desk Framework

No special Cross Functional projects have been identified for the Service Desk Framework. The project to implement the Service Portal is described in HPES' response to Schedule 2.1, Section 3.6.

Special Cross Functional Projects – Application Services Framework

Two special Cross Functional projects have been identified for the Application Services Framework. We illustrate these in Figure 145. .

Special Service Levels: Application Availability and Application Response Time. The process to implement these two Service Levels will be similar to that described above; however, since the ability to meet these Service Levels is predicated on each application's architecture capabilities and limitations, we are proposing an assessment during the Transition period of the ability of each application to meet these Service Levels. For example, in order to meet the Application Availability Service Level target, common industry practice is to have a high-availability architecture in place to prevent service outages in the event of hardware failures.

We will assess the applications to identify where they might have single points of failure that would prevent them from being eligible to meet these Service Levels, and present the County with a report of findings and recommendations. For any applications that require remediation, we will review these with the County to assist in determining the best-value response. For remediation plans approved by the County, we will submit a separate project schedule and estimate for completing the remediation of those environments. Once the remediation project is implemented for each application with gaps, the Service Level will take effect.

In the notional plan, we do not estimate a timeframe for completion of the remediation projects—only for submission of the plan. The schedule for readiness to assume this Service Level will depend on the number and scope of projects required, the County's other priorities, and the final determination of which applications to remediate and which to waive from the Service Level.

SaaS Application Onboarding: The County has identified in the solicitation 169 applications identified as SaaS applications that HPES does not currently support. For each of these that the County wishes us to support, we will need to perform the steps described in the Gantt chart above.

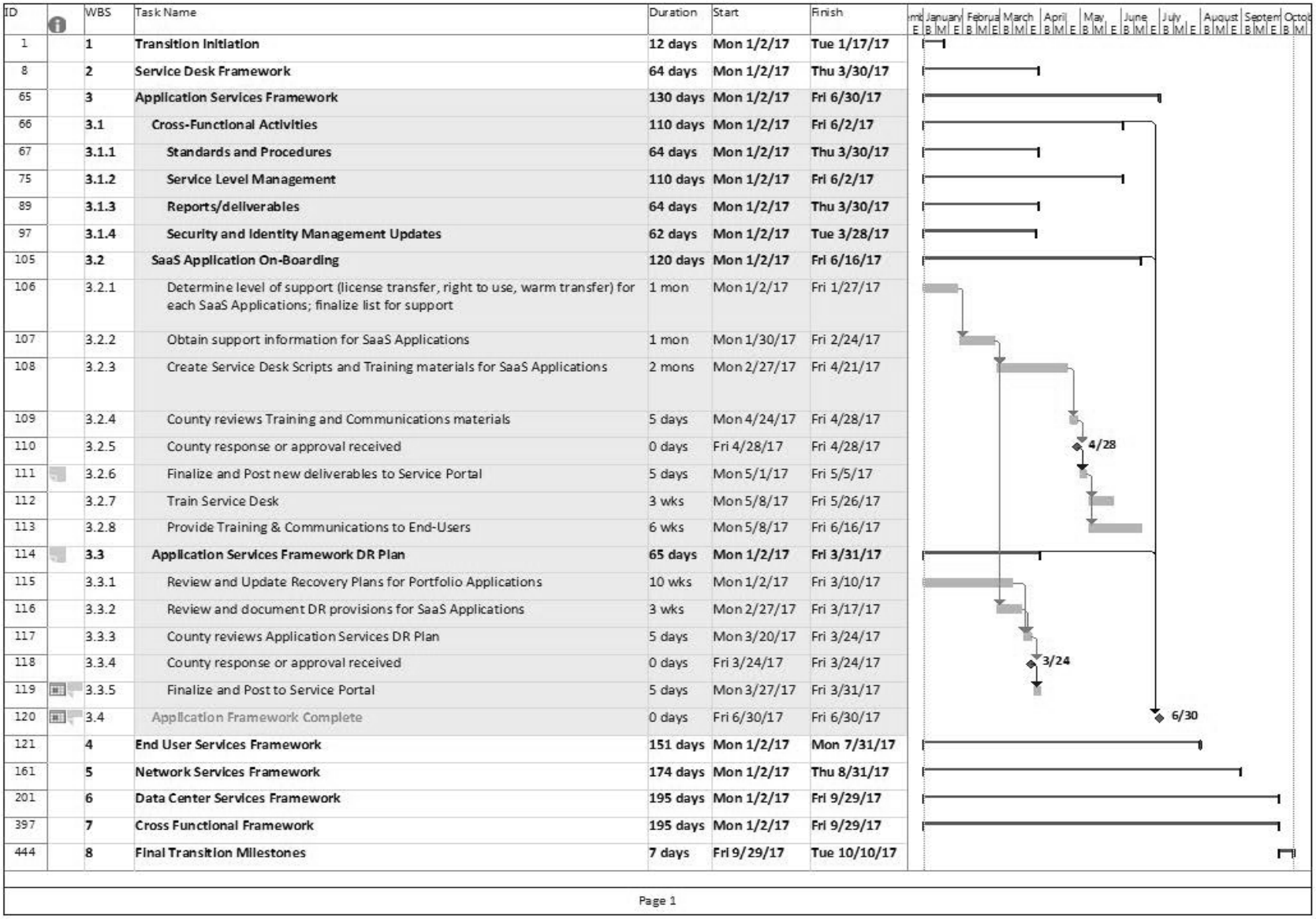
We will review each application that the County wants us to support, according to our established process for Third Party Agreements, and determine the level of support possible for each (license transfer, right to use, warm transfer). Once we have a final list, we will work with the support contacts at that vendor to understand their support process, and create Service Desk scripts that will enable our team to field those calls. We will then train our Service Desk staff to support them, and prepare communication materials for users of those applications to understand the new support process.

All draft materials will be submitted to the County for review and comment. The County will reply with any changes required within the agreed timeframe, after which we will finalize and post all deliverables to the Service Portal and cut over support for those applications during the Application Services Transition.

Special Cross Functional Projects – End User Services Framework

No special Cross Functional projects have been identified for the End User Services Framework.

Figure 145. Application Framework: SaaS Application Onboarding



ID	WBS	Task Name	Duration	Start	Finish
1	**1**	**Transition Initiation**	**12 days**	**Mon 1/2/17**	**Tue 1/17/17**
8	**2**	**Service Desk Framework**	**64 days**	**Mon 1/2/17**	**Thu 3/30/17**
65	**3**	**Application Services Framework**	**130 days**	**Mon 1/2/17**	**Fri 6/30/17**
66	**3.1**	**Cross-Functional Activities**	**110 days**	**Mon 1/2/17**	**Fri 6/2/17**
67	**3.1.1**	**Standards and Procedures**	**64 days**	**Mon 1/2/17**	**Thu 3/30/17**
75	**3.1.2**	**Service Level Management**	**110 days**	**Mon 1/2/17**	**Fri 6/2/17**
89	**3.1.3**	**Reports/deliverables**	**64 days**	**Mon 1/2/17**	**Thu 3/30/17**
97	**3.1.4**	**Security and Identity Management Updates**	**62 days**	**Mon 1/2/17**	**Tue 3/28/17**
105	**3.2**	**SaaS Application On-Boarding**	**120 days**	**Mon 1/2/17**	**Fri 6/16/17**
106	3.2.1	Determine level of support (license transfer, right to use, warm transfer) for each SaaS Applications; finalize list for support	1 mon	Mon 1/2/17	Fri 1/27/17
107	3.2.2	Obtain support information for SaaS Applications	1 mon	Mon 1/30/17	Fri 2/24/17
108	3.2.3	Create Service Desk Scripts and Training materials for SaaS Applications	2 mons	Mon 2/27/17	Fri 4/21/17
109	3.2.4	County reviews Training and Communications materials	5 days	Mon 4/24/17	Fri 4/28/17
110	3.2.5	County response or approval received	0 days	Fri 4/28/17	Fri 4/28/17
111	3.2.6	Finalize and Post new deliverables to Service Portal	5 days	Mon 5/1/17	Fri 5/5/17
112	3.2.7	Train Service Desk	3 wks	Mon 5/8/17	Fri 5/26/17
113	3.2.8	Provide Training & Communications to End-Users	6 wks	Mon 5/8/17	Fri 6/16/17
114	**3.3**	**Application Services Framework DR Plan**	**65 days**	**Mon 1/2/17**	**Fri 3/31/17**
115	3.3.1	Review and Update Recovery Plans for Portfolio Applications	10 wks	Mon 1/2/17	Fri 3/10/17
116	3.3.2	Review and document DR provisions for SaaS Applications	3 wks	Mon 2/27/17	Fri 3/17/17
117	3.3.3	County reviews Application Services DR Plan	5 days	Mon 3/20/17	Fri 3/24/17
118	3.3.4	County response or approval received	0 days	Fri 3/24/17	Fri 3/24/17
119	3.3.5	Finalize and Post to Service Portal	5 days	Mon 3/27/17	Fri 3/31/17
120	3.4	Application Framework Complete	0 days	Fri 6/30/17	Fri 6/30/17
121	**4**	**End User Services Framework**	**151 days**	**Mon 1/2/17**	**Mon 7/31/17**
161	**5**	**Network Services Framework**	**174 days**	**Mon 1/2/17**	**Thu 8/31/17**
201	**6**	**Data Center Services Framework**	**195 days**	**Mon 1/2/17**	**Fri 9/29/17**
397	**7**	**Cross Functional Framework**	**195 days**	**Mon 1/2/17**	**Fri 9/29/17**
444	**8**	**Final Transition Milestones**	**7 days**	**Fri 9/29/17**	**Tue 10/10/17**

Page 1

Special Cross Functional Projects – Network Services Framework

No special Cross Functional projects have been identified for the Network Services Framework. The re-architecture and refresh of the Tulsa Data Center network is described in the Data Center Consolidation Project (response to Schedule 2.1, Section 3.4).

Special Cross Functional Projects – Data Center Services Framework

A number of security projects have been identified for the Data Center Services Framework. These include the following:

- Projects to re-orient services that are active-active across sites in the two-data-center model, such as Active Directory, Active Directory Federation Services (ADFS), and the Endpoint Threat Protection core.
- Projects in support of the email transition to cloud, such as adaptation of the Security Incident Management process.
- Projects to address heightened security requirements, such as expansion of security information and event management (SIEM) services, design and implementation of a separate Development/Test network zone, and implementation of continuous scanning.
- As part of the Data Center network buildout, we will convert from Checkpoint firewalls with TippingPoint for intrusion detection/prevention services to Palo Alto devices that support both functions.

The Data Center related projects required by the RFP are addressed in the sections that respond to Schedule 2.1, Sections 3.2 (E-Mail), 3.3 (Development and Test Environment), 3.4 (Consolidated and Single Data Center), and 3.5 (Storage Architecture). The sub-project to implement the new Data Center DR architecture is also described in Section 3.4.

Special Cross Functional Projects – Replacement of myRequests

During the Cross Functional Transition, we will replace the current myRequests Service Request system with the Service Catalog and Request Manager that comes pre-integrated with HPE Service Manager. Because this migration will take longer than the Service Portal implementation, during the initial deployment of the Service Portal, the Service Portal will be linked (using a front page tile or from the "Links" tile, at the County's discretion) to the myRequests system, and we will maintain myRequests following our current processes, while the new request manager/service catalog functionality is being configured. Once the new Request Manager system is ready, and user training has taken place, we will disengage the link to myRequests and bring Request Manager online. Because the capabilities of myRequests cross multiple frameworks, we have included this project in the Cross Functional Framework.

Cross Functional Framework Transition: Activities Aligned to Framework Components

For the Cross Functional Framework components, the Transition follows the same basic structure as described above for the frameworks. Table 69 summarizes the approximate scope of change in each Cross Functional component. Upon analysis, the extent of change to each component has been categorized as follows:

- Limited – changes are expected to be minor updates to existing processes and deliverables
- Medium – some new processes or deliverables—generally similar to current practices
- Large – multiple new processes or deliverables—Organizational Change Management applies

Table 69. Approximate Scope of Change for each Cross Functional Component

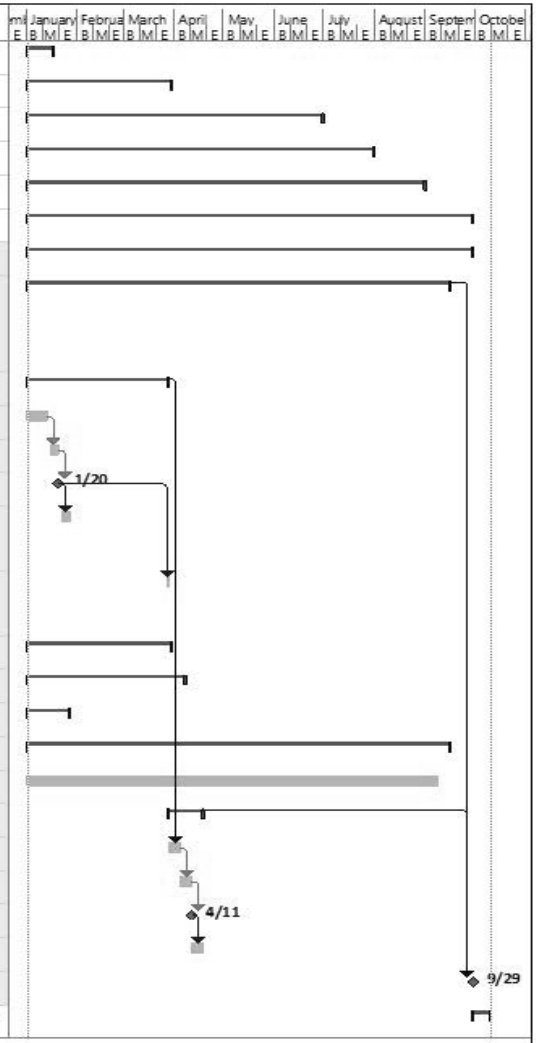
FRAMEWORK COMPONENT	EXTENT OF CHANGE	SPECIAL PROJECTS OR CONSIDERATIONS
Contract and Acquisition Management Services	Minimal	None
Integrated Asset Management Services	Limited	We will integrate data from AT&T Asset Management Systems
Billing Management Services	Limited	Setup of billing processes for new Resource Units
Security Management Services	Large	Multiple Security sub-projects within the Data Center and Network Frameworks, as described above.
Service Delivery Management Services	Medium	New component
Architecture Services	Medium	New component
Project Management Services	Limited	None
Integration and Testing Services	Medium	New component
Incident Management Services	Limited	New component
Problem Management Services	Limited	New component
Change Management Services	Limited	New component
Release Management Services	Medium	New component
Configuration Management Services	Limited	None
Capacity Planning and Performance	Medium	Metrics collection and reporting from new technologies: Helion Managed Private Cloud (MPC) and Helion Managed Cloud Broker (HMCB)
Disaster Recovery Management Services	Large	Implementation of new architectures and addition of Business Continuity specialists to the support team
Identity and Access Management Services	Large	Modification of AD and ADFS architectures to support a single data center model, automation of Access Management Workflows to replace the CSRF form,
Reporting Management Services	Large	Implementation of the Service Portal and Data Analytics will drive significant improvements in this area
Domain Name Management Services	Limited	None
Business Analyst Services	Medium	New Component

A notional project schedule for the Cross Functional Framework Transition is illustrated in Figure 146. This plan should be considered a "per-component" view—the actual project schedule would be exploded to include all components and the timeline expanded accordingly.

The basic steps for developing the Cross Functional Component Management Plan are the same as those for creating new procedures, described in the preceding section. Upon County approval, the Cross Functional Component Management Plans will be published on the Service Portal.

Figure 146. Cross Functional Framework – Component Management Plans

ID	WBS	Task Name	Duration	Start	Finish
1	1	**Transition Initiation**	12 days	Mon 1/2/17	Tue 1/17/17
8	2	**Service Desk Framework**	64 days	Mon 1/2/17	Thu 3/30/17
65	3	**Application Services Framework**	130 days	Mon 1/2/17	Fri 6/30/17
121	4	**End User Services Framework**	151 days	Mon 1/2/17	Mon 7/31/17
161	5	**Network Services Framework**	174 days	Mon 1/2/17	Thu 8/31/17
201	6	**Data Center Services Framework**	195 days	Mon 1/2/17	Fri 9/29/17
397	7	**Cross Functional Framework**	195 days	Mon 1/2/17	Fri 9/29/17
398	7.1	**Cross-Functional Activities (per Framework Component, many in parallel - timing for each framework component will vary based on the degree of change)**	185 days	Mon 1/2/17	Fri 9/15/17
399	7.1.1	**Cross-Functional Component Management Plan**	62 days	Mon 1/2/17	Tue 3/28/17
400	7.1.1.1	Develop Cross-Functional Component Management Plan	2 wks	Mon 1/2/17	Fri 1/13/17
401	7.1.1.2	County reviews Cross-Functional Component Management Plan	5 days	Mon 1/16/17	Fri 1/20/17
402	7.1.1.3	County response or approval received	0 days	Fri 1/20/17	Fri 1/20/17
403	7.1.1.4	Finalize, Implement and deliver the Cross-Functional Component Management Plan	5 days	Mon 1/23/17	Fri 1/27/17
404	7.1.1.5	Post the Cross-Functional Component Management Plan to the Service Portal	1 day	Tue 3/28/17	Tue 3/28/17
405	7.1.2	**Standards and Procedures**	64 days	Mon 1/2/17	Thu 3/30/17
413	7.1.3	**Service Level Management**	70 days	Mon 1/2/17	Fri 4/7/17
421	7.1.4	**Reports/deliverables**	20 days	Mon 1/2/17	Fri 1/27/17
429	7.1.5	**Security and Identity Management Updates**	185 days	Mon 1/2/17	Fri 9/15/17
437	7.2	Implement new OIC / Service Request Manager (replace myRequests)	180 days	Mon 1/2/17	Fri 9/8/17
438	7.3	**Cross Functional DR Plan**	15 days	Wed 3/29/17	Tue 4/18/17
439	7.3.1	Review and Update Cross Functional DR Plan	5 days	Wed 3/29/17	Tue 4/4/17
440	7.3.2	County reviews Cross Functional DR Plan	5 days	Wed 4/5/17	Tue 4/11/17
441	7.3.3	County response or approval received	0 days	Tue 4/11/17	Tue 4/11/17
442	7.3.4	Finalize and Post to Service Portal	5 days	Wed 4/12/17	Tue 4/18/17
443	7.4	Cross-Functional Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17
444	8	**Final Transition Milestones**	7 days	Fri 9/29/17	Tue 10/10/17



Page 1

- Automated Tools – Automated systems and tools involved in proposed solution

Information feeds from various operational tools will be used to provide Cross Functional Service deliverables.

No tools beyond those already described for managing the Transition process are required to transition the Cross Functional Framework.

- Qualifications and Experience – Background and experience in comparable environments

The best indicator that we will be successful is that we have done this before for the County. We provide several highlights from our current County service and similar engagements in Table 70.

Table 70. Similar Engagements

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND HOW IT IS RELEVANT TO THE COUNTY
County of San Diego	Performed successful transition from Northrop Grumman in 2011, including transition of Cross Functional Services.
Next Generation Enterprise Network	On the Department of Navy (DON), Next Generation Network (NGEN) Contract which includes support for Navy Marine Corps Intranet (NMCI). HPE is on our second term of this Contract. We successful transitioned from the prior to current Contract including in many cross-functional component areas.
Multi-Supplier Integration Services (MSI) for Procter and Gamble (P&G)—also known as Operations Integration Service (OIS)	• MSI and OIS are part of the June 2012 renewal contract with HP Enterprise Services to support P&G's "always-on" operating environment in driving greater transparency and consistency across P&G and its technology partners by providing standard tools, processes, and an integrated dashboard. • Upon renewal, HPES transitioned all services and cross-functional activities.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (optional) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

E-Mail Services (Schedule 2.1, Section 3.2)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary

HPES has been delivering email services to the County of San Diego for 10 years. Our understanding of your environment, needs and vision, led to the conclusion that rather than upgrading your existing Exchange 2010 environment, we will move the County to Office 365 Exchange Online.

Our transition approach is simple. As with previous email migrations, we will work with CTO to identify the move groups, determine success criteria and finalize timing. Next, we will execute a proven HPE methodology, Migration Factory (MF). MF is a standardized service that uses specialized tools running on temporary servers to move email boxes from traditional Exchange servers to the Microsoft Office 365 Government Community Cloud. We expect to move County users in waves from Exchange to the MS Cloud over an 8 to 10 week period.

It is essential to your email users that they have access to their non-inbox PSTs. These are generally archive PSTs but can include others as well. The email migration described above covers those emails that are in the current inbox. HPES will, in a separate PST Migration Project, migrate users' PST files to their Exchange Online Mailbox. The PST Migration Project is expected to parallel that of the inbox migration and complete at approximately the same time.

Rationale

We fully understand the importance of maintaining uptime of the current email services. We will continue to manage the current Exchange 2010 environment until such time as all users are moved. The Service Desk will own tickets from start to finish in support of both Exchange and Office 365 environments.

We are proposing this now because it reduces the need for hosted server-based solutions and allows for the efficiency and flexibility of a cloud-based offering. We also feel that moving to MS Cloud is more in line with the stated future technology direction of the County.

This migration will be accomplished prior to the end of the Transition Period, negating the need to upgrade your existing Exchange 2010 environment, allowing the data center based email infrastructure to be retired when the migration is complete.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Members of our U.S. Messaging Practice, in coordination with CTO, will both plan and execute the migration, with support from the local HPES who provide institutional knowledge of the current environment. A transition project manager will guide the entire process, and County users will be supported by the HPES Service Desk.

HPES will complete the migration virtually and at the Plano and Tulsa data centers. We are unique in the industry since we also have support personnel co-located in Redmond, WA at Microsoft headquarters. Microsoft engineers will use the County ticketing system to support trouble tickets during the migration and provide experts to resolve issues if needed.

The County's Office 365 environment will reside in the Microsoft Office 365 Government Community Cloud environment, this a hardened U.S.-based environment that is FedRAMP authorized, and whose support personnel are appropriately screened. It has features that can support Criminal Justice Information Services (CJIS) requirements for law enforcement agencies, and IRS-1075 requirements for customers who handle Federal Taxpayer Information (FTI).

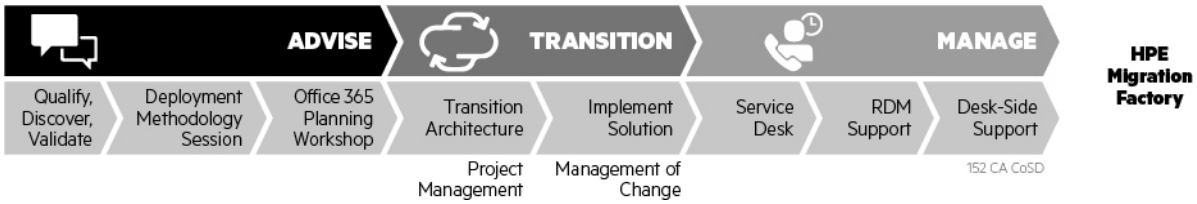
- Methodology & Key Processes – Key methodologies and processes in proposed solution

HPES' dedicated E-Mail migration practice is built on standard processes, tools, and trained personnel to assess, prepare, implement, and then decommission Exchange. We have a repeatable process that HPES

has developed through its migration expertise (including our own experience migrating over 300,000 mailboxes to Office 365

The Office 365 transformation methodology follows our standard advise, transition, and manage approach that closely follows the County's plan, build, operate formula see Figure 147. Messaging engineers will provide due diligence on the current environment, and prepare the infrastructure and tools that the Migration Factory personnel will use to move from Exchange 2010 to Exchange Online.

Figure 147. HPES' Advise, Transition and Mange Approach

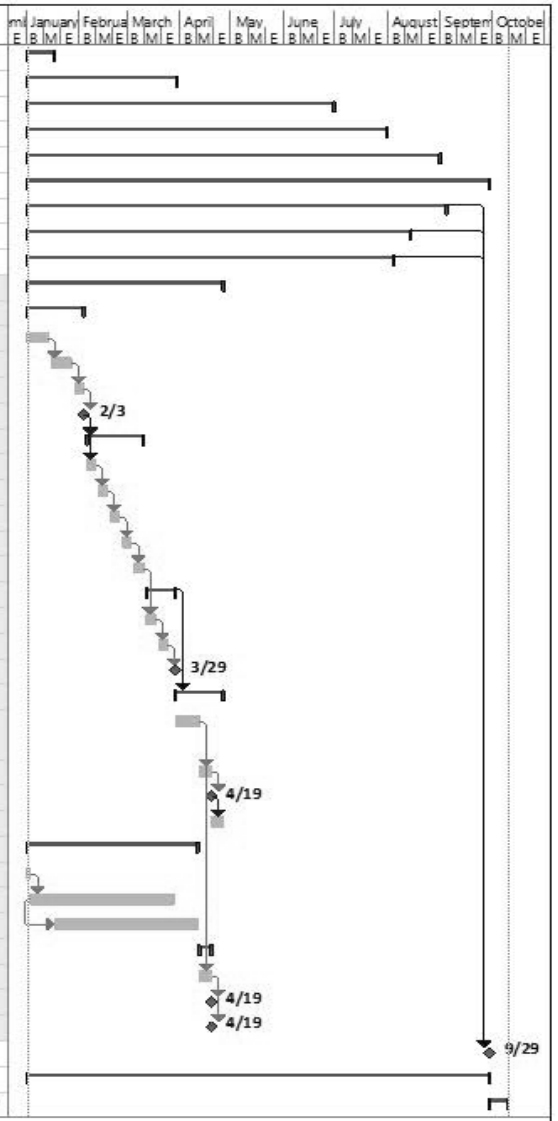


Transition Schedule and Tasks

Figure 148 presents a notional transition schedule and Gantt chart, with high level tasks and milestones based on a January 2, 2017, Contract Effective Date (CED). The schedule is easy to adjust based on the actual CED. HPES will provide the final E-Mail Transition Plan and Schedule for County approval. Task descriptions and key milestones are discussed in detail below.

Figure 148. E-MAIL Migration Tasks

ID	WBS	Task Name	Duration	Start	Finish
1	1	**Transition Initiation**	12 days	Mon 1/2/17	Tue 1/17/17
8	2	**Service Desk Framework**	64 days	Mon 1/2/17	Thu 3/30/17
65	3	**Application Services Framework**	130 days	Mon 1/2/17	Fri 6/30/17
121	4	**End User Services Framework**	151 days	Mon 1/2/17	Mon 7/31/17
161	5	**Network Services Framework**	174 days	Mon 1/2/17	Thu 8/31/17
201	6	**Data Center Services Framework**	195 days	Mon 1/2/17	Fri 9/29/17
202	6.1	**Cross-Functional Activities**	176 days	Mon 1/2/17	Mon 9/4/17
235	6.2	**Data Center Services DR Plan and DR Architecture Implementation**	161 days	Mon 1/2/17	Mon 8/14/17
251	6.3	**Data Center Framework Transition Projects**	155 days	Mon 1/2/17	Fri 8/4/17
367	6.4	**Email Services**	83 days	Mon 1/2/17	Wed 4/26/17
368	6.4.1	**Plan and Design**	25 days	Mon 1/2/17	Fri 2/3/17
369	6.4.1.1	Develop Migration Plan	2 wks	Mon 1/2/17	Fri 1/13/17
370	6.4.1.2	Design Migration Infrastructure	2 wks	Mon 1/16/17	Fri 1/27/17
371	6.4.1.3	County Reviews Email Migration Plan and Design	5 days	Mon 1/30/17	Fri 2/3/17
372	6.4.1.4	County response or approval received	0 days	Fri 2/3/17	Fri 2/3/17
373	6.4.2	**Configure**	25 days	Mon 2/6/17	Fri 3/10/17
374	6.4.2.1	Configure Migration Tool Virtual Server	1 wk	Mon 2/6/17	Fri 2/10/17
375	6.4.2.2	Deploy Migration Tool	1 wk	Mon 2/13/17	Fri 2/17/17
376	6.4.2.3	Configure DNS and Network	5 days	Mon 2/20/17	Fri 2/24/17
377	6.4.2.4	Deploy Hybrid Server	1 wk	Mon 2/27/17	Fri 3/3/17
378	6.4.2.5	Perform System Integration Test	5 days	Mon 3/6/17	Fri 3/10/17
379	6.4.3	**Pilot Program**	13 days	Mon 3/13/17	Wed 3/29/17
380	6.4.3.1	Perform Production Pilot Migration	5 days	Mon 3/13/17	Fri 3/17/17
381	6.4.3.2	Conduct User Acceptance Testing	5 days	Mon 3/20/17	Fri 3/24/17
382	6.4.3.3	Review results; Obtain County Approval to Proceed	3 days	Mon 3/27/17	Wed 3/29/17
383	6.4.4	**Documentation and Training**	20 days	Thu 3/30/17	Wed 4/26/17
384	6.4.4.1	Update Service Documentation, Training and Service Desk scripts	2 wks	Thu 3/30/17	Wed 4/12/17
385	6.4.4.2	County reviews Final Documentation	5 days	Thu 4/13/17	Wed 4/19/17
386	6.4.4.3	County response or approval received	0 days	Wed 4/19/17	Wed 4/19/17
387	6.4.4.4	Finalize documents, Post to Service Portal	5 days	Thu 4/20/17	Wed 4/26/17
388	6.4.5	**Migration Waves**	72 days	Mon 1/2/17	Tue 4/11/17
389	6.4.5.1	Define Migration Waves in coordination with CTO	2 days	Mon 1/2/17	Tue 1/3/17
390	6.4.5.2	Execute Migration Waves	12 wks	Wed 1/4/17	Tue 3/28/17
391	6.4.5.3	PST Migration	12 wks	Wed 1/18/17	Tue 4/11/17
392	6.4.6	**Project Completion**	5 days	Thu 4/13/17	Wed 4/19/17
393	6.4.6.1	Obtain Final County Approval and Signoff	5 days	Thu 4/13/17	Wed 4/19/17
394	6.4.6.2	County Approval Received	0 days	Wed 4/19/17	Wed 4/19/17
395	6.4.6.3	Email Services Migration Complete	0 days	Wed 4/19/17	Wed 4/19/17
396	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17
397	7	**Cross Functional Framework**	195 days	Mon 1/2/17	Fri 9/29/17
444	8	**Final Transition Milestones**	7 days	Fri 9/29/17	Tue 10/10/17



Page 1

PST Migration will follow a similar high-level methodology but with a simpler work breakdown. The basic process for PST Migration is as follows:

- PST Discovery: PST files are scattered among file shares and even local disk drives of end users. They will be found via domain-level discovery of user shares and drives.
- PST Harvesting: Those files are then gathered in a central filestore, linked to the user's Exchange Online account, and readied for import.
- PST Transfer: Whereas PSTs can be imported to Exchange Online via transfer over the WAN, for the large number of mailboxes and potentially large data sets, we will use Microsoft's Import Service via drive shipping. The data sets are stored on an encrypted drive and transported to Microsoft for import. This significantly reduces the amount of time for WAN transport of 15,000+ separate PST files.
- PST Import: Microsoft will import the users' PSTs to their individual Archive Mailboxes. There is no size limit to the amount of emails that may be stored in Archive Mailboxes.

Plan and Design. For the Email Migration project, during the planning period, we will create the detailed migration plan and present it to the County for review and approval. As part of this process, the U.S. Messaging Practice, with advisement from the current email support staff, will assess the environment, size the migration temporary infrastructure needs, and mitigate any potential or actual issues. Because the County's Active Directory system is already integrated with Microsoft Active Directory Federation Services (ADFS) in the cloud, this provides a significant benefit for the migration.

Configure. HPES will set up temporary infrastructure, configure the migration tool virtual server, configure DNS and network, and deploy a hybrid server. After system integration testing is successfully completed, we will be ready to perform a pilot launch.

Pilot Program. The Migration Factory will perform a pilot migration on a subset of users defined by CTO, moving them to Office 365 and seeking feedback on their experience. We will conduct UAT in collaboration with the County, review results, and adjust our plan as needed based on the results and user feedback.

Documentation and Training. We will prepare service documentation, training materials, and Service Desk scripts to prepare for the migration waves. The County will review the deliverables, HPES will respond to questions or clarifications, and then seek final approval to proceed. The completed documents and training material will be added to the Service Portal, and we will train our Service Desk agents and other support personnel. We will review with CTO to determine if other types of training may be required and deliver that training accordingly.

Migration Waves. Our Migration Factory will then begin executing the migration move groups moving each group's mailboxes from the Exchange servers to the Microsoft Office 365 Government Community Cloud. We expect the migration to take place during an 8–12 week period. As groups are migrated in waves, we will move into the manage phase, providing support.

Project Completion. HPES will request final County approval and sign-off. After all users are migrated and County approval is received, the E-Mail migration will be complete. Similarly, after all PSTs have been migrated to users' archived mailboxes, the PST Migration will be complete.

- Automated Tools – Automated systems and tools involved in proposed solution

To accomplish migration, we use HPES internally developed software and a migration tool from Binary Tree Company. We use a utility available from Microsoft for migrating PSTs.

Table 71. Automated Tools

TOOL NAME AND VENDOR	DESCRIPTION
E2E by BinaryTree Corporation	• Analysis and migration engine for migrating on premise Exchange mailboxes to Exchange Online • Allows rapid, low-risk migrations of large Exchange user populations. • This is the preferred tool of HPES messaging engineers
PST Capture	• Microsoft tool for searching and harvesting PST files

- Qualifications and Experience – Background and experience in comparable environments

We have migrated thousands of Exchange mailboxes to Office 365, including the entire user population of Hewlett Packard (HPE/HP Company combined), and many other commercial and U.S. Public Sector clients, for a total of more than 800,000 seats. This experience, combined with the institutional knowledge of the County infrastructure, significantly reduces the transition risk. The resources who led our own migration now leads our U.S. Messaging Practice, which will perform the County's migration to Office 365 Exchange Online.

Table 72. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND RELEVANCY TO THE COUNTY
County of San Diego	HPES successfully migrated the County to Exchange 2010 in 2012. This included migrating 14,125 mailboxes spread across 4 clustered mailbox servers in 2 data centers, configuring ActiveSync, and providing the County the ability to perform E-mail journaling for mailbox special investigations. We also support mobile device management, using AT&T's AirWatch tool, and two RightFax servers with a total of 203 active users. Since Migrating to Exchange 2010, the County has experienced no Severity 1 or Severity 2 service interruptions. The environment is extremely reliable, providing County user's quality service and customer satisfaction.
Hewlett Packard Enterprise	HPE completed its own internal move to E-mail in the cloud. More than 300,000 mailboxes have been moved to Office 365 (HPE/HP Company combined) using the same process we propose for the County.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (optional) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

Development and Test Environment (Schedule 2.1, Section 3.3)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Transition of the existing Development and Test (Dev/Test) environment is a critical element of the data center consolidation effort, which is fully described in the Transition Projects: Consolidated and Single Data Center, in response to Schedule 2.1, Section 3.4. Many of the steps to accomplish the Dev/Test transition are described within the overall data center consolidation project because this is such an integral part of the project. This section will primarily describe those activities unique to Dev/Test.

Solution Summary

Our solution for Dev/Test is tightly linked to the data center consolidation and the evolution of the Data Center to a hybrid environment: it uses the Helion Managed Private Cloud (MPC), as described in the Data Center Consolidation Transition Project, and Helion Managed Cloud Broker (HMCB) to provide a business-rule defined boundary for Dev/Test capacity. This allows the environment's composition of server sizes and platforms in the hybrid environment to evolve and change over time in response to changing requirements without exceeding the County's established financial parameters. We will define thresholds to warn when the environment is approaching those limits.

HPES will provide a persistent Dev/Test environment for all P1 and P2 applications, so that high-priority County applications are guaranteed the resources needed to conduct testing in support of production issues (Applications Maintenance and Operations) or development projects with an urgent timeframe. We will also maintain surplus space in the Dev/Test environment beyond that needed for the P1 and P2 applications to accommodate non-persistent Dev/Test capabilities for P3 through P5 applications. The surplus space will be used on an as-needed basis to support the normal development and test activities of these lower-priority County applications. This approach controls the cost of the overall Dev/Test environment while also providing ample capacity for the County's suite of applications.

We will manage Dev/Test workloads within a SAN-based repository visible to the private cloud and perform tasks such as boot up and shutdown of virtual machine images on demand. Upon the County's request/approval, tasks will commence automatically. The Dev/Test environment will have interfaces enabling connectivity to the Production environment to meet business needs. We will secure these interfaces with virtual local area networks (VLANs) and access control lists (ACLs). Identity access management services will be applied across all County environments, including Dev/Test. These services are described further in our response to Schedule 4.3, Section 2.18 contained in Section 2.5 of this proposal.

We will implement the HPE Codar toolkit to create an automated Release Management Framework in the Dev/Test environment. This will support the evolution of our Applications Development Services to adoption of DevOps practices.

A complete description of the Dev/Test environment is included in Section 2.9 of this proposal in response to Schedule 4.3, Section 6.9.

Rationale

Transition to MPC and HMCB will provide an integrated platform for Dev/Test services that mimics the Production environment to streamline application development and deployment. HMCB provides the tools to create the hybrid design that the County is looking for in this environment. These tools provide the flexibility to include or exclude any type of platform within the Dev/Test scope, and manage its size based on a financial and business viewpoint instead of having to be concerned about the exact mix of

hardware and software. We can make this definition all-inclusive or create the business rules to be less flexible according to the County's preference, without impacting the project timeline or plan. As the County's environment becomes more standardized, we can collaborate to adjust the Dev/Test environment parameters to suit evolving requirements without reconfiguring the underlying technologies.

Because these tools are used to support applications in both Dev/Test and Production and are a key component of the Data Center Services Framework, transition of Dev/Test is designed to occur in conjunction with the remainder of the framework.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The Data Center Consolidation Transition Project Manager (TPM) will be directly responsible for activities associated transition of the Dev/Test environment. The Data Center Consolidation TPM will be supported by the Cloud Services TPM, responsible for the MPC and HMCB services portion of the Transition. Our virtual support team includes architects, engineers, and migration specialists with expertise in cloud services and experience building out these environments for other clients. Additional details on Transition staffing are provided in Section 2.11, Requirements, in response to Schedule 2.1, Section 2.

The existing data center facilities in Tulsa and Plano are required to support transition of Dev/Test until migration of all workloads is complete.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

Methodologies and key processes for the Dev/Test Transition are the same as those described in response to the Data Center Consolidation Transition Project.

Transition Schedule and Tasks

The Data Center Consolidation Transition Plan, shown in Figure 149, includes the activities required for the Dev/Test environment transition to the hybrid cloud; these are described as part of the Data Center Consolidation Transition Project. Those tasks unique to the Dev/Test environment begin where we configure the HMCB to establish virtual boundaries for the Dev/Test environment and other resource pools as needed. The preceding tasks are shown for context.

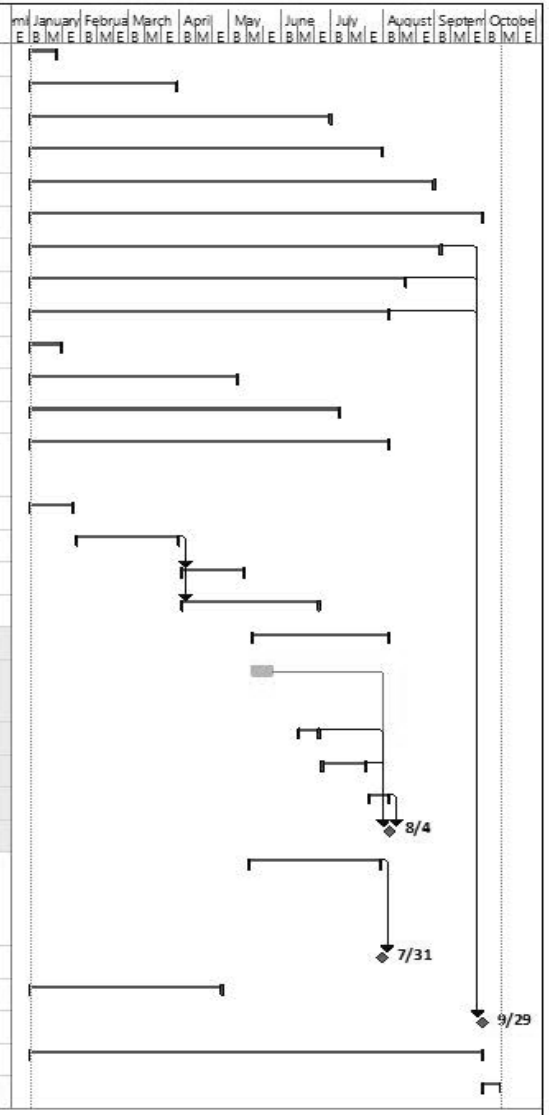
Planning and Build Phases (described in response to Section 3.4). During the Consolidation Assessment task, we will build a migration roadmap detailing the placement, plan, design, and execution of migrations of development and testing workloads currently residing in Tulsa and Plano.

Once the hybrid architecture is built out, the HPES engineering and applications team will collaborate with the County to define and size the composition of the Dev/Test portion of the environment, defining the financial parameters for each type of environment to be included. Dev/Test traditional servers already resident in Tulsa will be included immediately; as servers from Plano migrate into the environment, they will be imported into HMCB.

HPE Codar Environment Tasks. Once the Dev/Test environment is defined and built, we will design the environment for automated release management. This will include design and configuration of the infrastructure, implementation of the software tools and necessary processes to manage them, and testing with a sample application.

Figure 149. Dev/Test Transition within Data Center Consolidation

ID	WBS	Task Name	Duration	Start	Finish
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17
235	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17
252	6.3.1	Define High Level Plan	15 days	Mon 1/2/17	Fri 1/20/17
260	6.3.2	Data Center Network Architecture - Refresh and Expansion	90 days	Mon 1/2/17	Fri 5/5/17
277	6.3.3	Storage Architecture	133 days	Mon 1/2/17	Wed 7/5/17
298	6.3.4	Data Center Hybrid Architecture (Includes Dev/Test Environment) & Consolidation to Tulsa	155 days	Mon 1/2/17	Fri 8/4/17
299	6.3.4.1	Consolidation Assessment	20 days	Mon 1/2/17	Fri 1/27/17
303	6.3.4.2	Design and Procure Target Server Environment	45 days	Mon 1/30/17	Fri 3/31/17
309	6.3.4.3	Design Migration Plan	27 days	Mon 4/3/17	Tue 5/9/17
316	6.3.4.4	Build out Hybrid Environment	60 days	Mon 4/3/17	Fri 6/23/17
325	6.3.4.5	Development and Test Environment Configuration	60 days	Mon 5/15/17	Fri 8/4/17
326	6.3.4.5.	Configure HMCB Financial Governance for Development and Test Environment boundaries	2 wks	Mon 5/15/17	Fri 5/26/17
327	6.3.4.5.	HPE Codar Design and Engineering	10 days	Mon 6/12/17	Fri 6/23/17
333	6.3.4.5.	HPE Codar Implementation	20 days	Mon 6/26/17	Fri 7/21/17
339	6.3.4.5.	Testing and Go-Live	10 days	Mon 7/24/17	Fri 8/4/17
344	6.3.4.5.	Development and Test Environment Configuration Complete	0 days	Fri 8/4/17	Fri 8/4/17
345	6.3.4.6	Execute Migration move groups (Actual order, timing and number of move groups will be based on application dependencies and County priorities)	89.47 days	Fri 5/12/17	Mon 7/31/17
366	6.3.4.7	Consolidated Data Center Complete	0 days	Mon 7/31/17	Mon 7/31/17
367	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17
396	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17
397	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17



Page 1

Migration to Dev/Test (described in response to Section 3.4). HPES migration engineers will coordinate closely with the Application Development team to be aware of in-flight projects and migrate these at the proper time, in a non-disruptive manner.

We will prioritize move groups, with Plano workloads coming into Tulsa having the highest priority. This will allow the County to consolidate into Tulsa as quickly as possible, to meet consolidation objectives. We will migrate all remaining non-production workloads into the Dev/Test environment (either by actual migration into the MPC or by including them in the virtual boundary created by the HMCB).

- Automated Tools – Automated systems and tools involved in proposed solution

HPES will use the same automated tools as described in Section 2.11, Consolidated and Single Data Center, in response to Schedule 2.1, Section 3.4.

- Qualifications and Experience – Background and experience in comparable environments

HPES brings more than 40 years' experience in data center transition and consolidation with a special emphasis on collaboration to add value. We will leverage our industry best practices, deep IT expertise, and trusted, reliable, and repeatable services on behalf of the County. HPES delivers solutions that we know will work, are time-tested, and produce expected results.

Seadrill: For Seadrill, an offshore oil drilling company, HPE migrated to a more flexible delivery model for the infrastructure to keep up with growth and accommodate moving corporate offices and IT operations. This migration included Development and Test environments. Seadrill's objectives included the following:

- Vacate existing data center facility in 6 months
- Move data and IT into an Infrastructure-as-a-Service (IaaS) with capacity on demand
- Provide disaster recovery

To support Seadrill's objectives, HPES performed an end-to-end integration and migration into one of its Managed Cloud environments including operating systems and applications. The effort involving hundreds of Seadrill applications and servers, and conducted in close collaboration with other Seadrill vendors, was completed on-time and within budget. As a result of HPES's efforts, Seadrill realized the following benefits:

- Successful migration to the cloud
- Flexible, cost-effective multi-supplier IT environment
- Ability to keep up with at least 5% growth per year in servers and 20% in storage
- High availability (99.9%) plus disaster recovery

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

Please refer to the price volume for discussion of an alternative pricing approach for Dev/Test.

Consolidated and Single Data Center (Schedule 2.1, Section 3.4)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary

In support of the County's objective to consolidate two existing data centers—Plano, TX and Tulsa, OK––and institute a new Disaster Recovery (DR) program, HPES developed our data center consolidation transition plan to accommodate these changes and minimize disruption to ongoing services. With the consolidation, Tulsa will become the single production data center, and we will migrate all services from Plano to Tulsa. We will build a DR environment for the County at the HPES DR site in Colorado Springs, CO. It will provide failover capability for applications that require DR (generally the P1/P2 applications), core services, and data center security services. The data center consolidation will contribute to a unified strategy for the County, leading to improved operational efficiencies through a single data center services model and DR site.

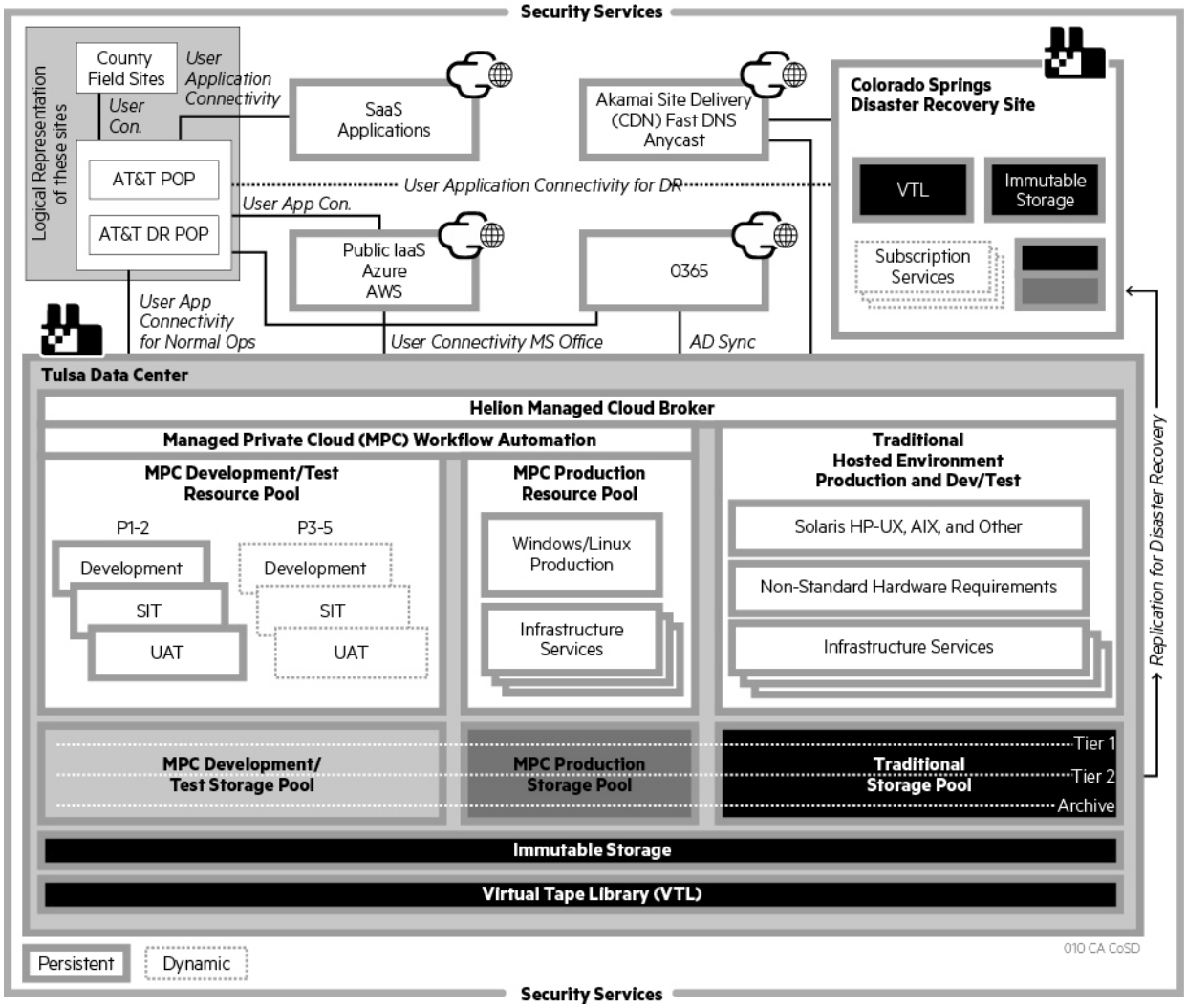
Our structured transition approach for the data center consolidation is comprised of the following subprojects. These will be completed in the sequence listed below to accomplish a smooth and nondisruptive transition.

- Set up and configure the data center network and security infrastructure to meet the new requirements.
- Refresh the data center storage environment to meet the requirements of Schedule 2.1, Section 3.5, (as described in Section 2.11, Storage Architecture, in response to that requirement)
- Build out the hybrid management capability and prepare the Tulsa data center to receive the server capacity currently resident in Plano. These activities will be performed in parallel with the instantiation of the DR capability, and will include the subproject to set up the development and test (Dev/Test) environment. The latter project is described in detail in Section 2.11, Development and Test Environment, in response to Schedule 2.1, Section 3.3.
- Migrate applications, and in some cases, equipment, from Plano to Tulsa, based on a move group schedule mutually define by HPES and the County.
- Migrate the County's mail presence from the current Exchange environment to the Microsoft Azure Government instance of Office 365. Note that this project is not dependent on the ones above—it can be executed before or in parallel with them—but must be completed before the Plano environment can be decommissioned. This project is described in detail in Section 2.11, Email Services, in response to Schedule 2.1, Section 3.2.

For each component identified above, HPES will provide a specific transition plan, interlocked with its related plan and the master schedule that details the tasks, milestones and schedule, for approval by the County. Throughout the project, we will work collaboratively with the County to develop success criteria, validate the scope and deliverables, and provide regular communication of the project's status, anticipated risks or issues, and our mitigation approach to make sure potential problems do not interfere with project completion.

Figure 150 provides an overview of the consolidated data center post-transition. A detailed description of each component of the data center is included in Section 2.9 of this proposal. Following Figure 151 we briefly describe each component of the consolidated data center associated with the transition.

Figure 150. Consolidated Data Center Overview

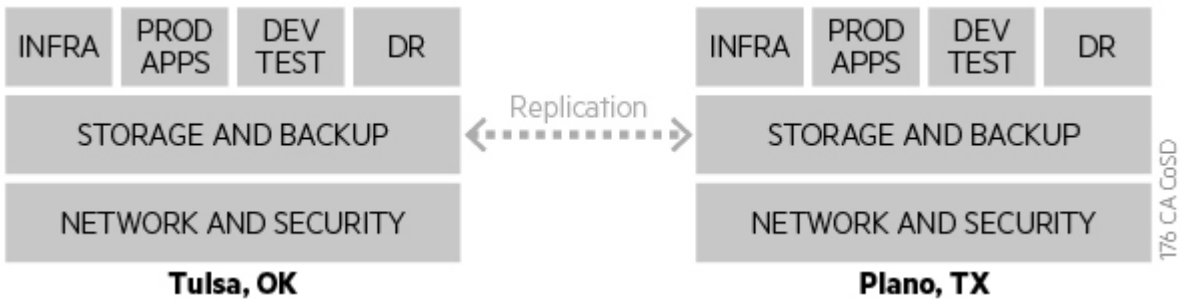


The Data Center Consolidation will result in a modern hybrid environment.

Data Center Consolidation – Overview of Steps

The figures that follow describe the high-level steps for the consolidation project. Figure 151 depicts the County Data Center environment (Plano and Tulsa only), showing the basic classifications of servers and infrastructure as they are in place today.

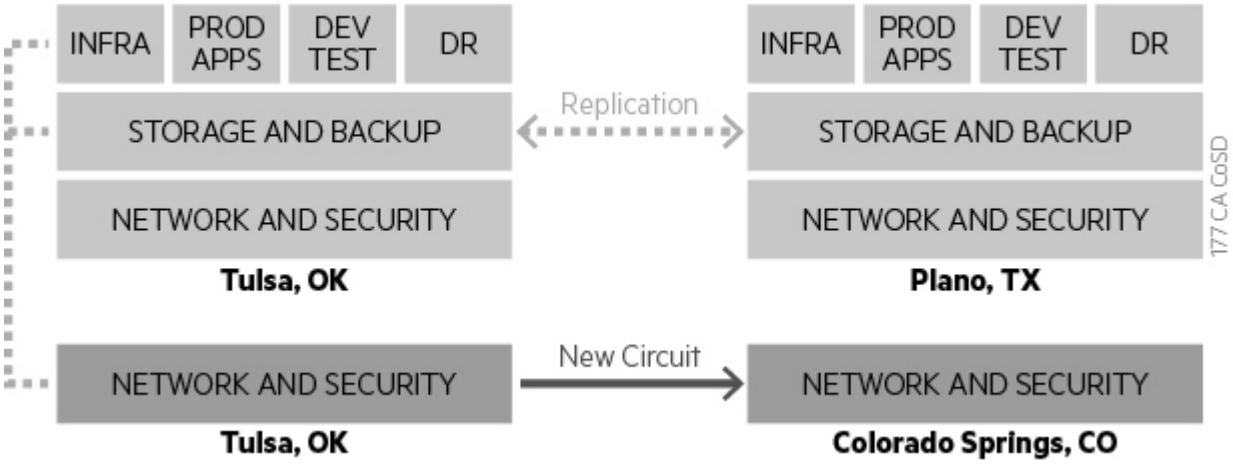
Figure 151. Current Data Center Environment



The first step, shown in Figure 152, will be to build out the new Data Center network compartment with the new network and security components. The new network compartment in Tulsa will be built out in the same physical room as the current Tulsa environment. Its components are described in Figure 153 and in additional detail in Section 2.9. In parallel with the Tulsa network buildout, we will build out the network compartment for the DR environment in Colorado Springs.

The process to refresh/replace the network environment will follow an "A/B" migration approach. We will build out the new network infrastructure (e.g., loadbalancers, firewalls, switches, routers) reproducing the existing configurations on the new equipment. When we have tested and verified the configurations, we will take a change window to shut down the "A" side of the environment (all traffic will seamlessly fail over to the "B" side), and bring up the new equipment's "A" side. We will reroute the traffic to the new equipment and verify proper operation. Once we are certain that no failback is needed, we replace the "B" side of the equipment with the new equipment (again, in a controlled change window), re-test the failover, and once all is operating correctly, remove the old equipment.

Figure 152. New Network Compartments in Tulsa and Colorado Springs



Internet Connection. Leveraged Internet Service (LIS) provides shared Internet connections in a multi-tenant data center. HPES obtains and manages the Internet connectivity to the data-center itself, and then extends that connectivity to applications in the data-center. Each LIS core router is each connected (using link-aggregation) to both of the two WAN connectivity Layer-Aggregation Switches (WCL-AS) for the data center. Each LIS core router also terminates a connection from an Internet Service Provider (ISP). The WCL-AS connections will provide the path to the downstream LIS customer environment.

WAN Connectivity. The HPES data center will be connected to the DR site using Ethernet MPLS WAN connectivity to provide high-speed data transmission, connecting back into the County's Points of Presence (POP). Connectivity will be sized to 250Mbps of bandwidth with the capability to increase up to 1Gbps. We will have the capability of meeting any annual bandwidth increases should the County require. Within the HPES data center, our support team will manage the dedicated WAN devices. Within the County POPs, AT&T will manage the dedicated WAN devices. All network traffic between the data center and the POPs will be encrypted.

With a focus on steady, progressive change, the County has increased network reliability and reduced single points of failure. This resilient architecture will serve as the foundation for the County's future network. The network design associated with the consolidated data center addresses some limitations associated with the current network architecture to facilitate rapidly growing bandwidth and storage needs, reducing the complexity of the infrastructure, delivering high availability (HA), redundancy. This will reduce the manually intensive processes and provide the convergence of networking and storage

fabrics. It also contains standard 10Gbps and 1Gbps capabilities for attached devices, including servers, firewalls, and IPS devices. It is designed with virtualization and automation in mind and provides a foundation for a converged infrastructure.

The network will provide a redundant topology to eliminate network downtime by a single point of failure. Our network design will provide redundancy for enhanced reliability with multiple connections to network devices. Network reliability is achieved through reliable equipment and network designs that are tolerant to failures and faults by reconverging rapidly to bypass faults when these occur. On a redundantly connected network, if a router fails, connectivity is preserved by routing traffic through a redundant connection. Furthermore, each router has two or more points, or "legs," to provide additional redundancy.

Our design within the data center will flatten the layer 2 architecture and provide a low cost capacity switching fabric. This is done through the adoption of a spine and leaf topology (2-tier) network design. The L2Spine is a high speed connection between any devices attached to the leaf nodes. It eliminates unused network links and introduces full throughput on all connections between network devices using HPES networking technology known as Intelligent Resilient Framework (IRF). Using IRF, multiple switches are grouped and appear as a single logical device that allows all links connected to these devices to forward traffic in a loop-free topology. Each device is fully redundant. IRF provides a non-blocking architecture within the layer 2 network fabric. It enables highly efficient high-bandwidth connectivity and N +1 redundancy. It provides up to 40Gbps of server connectivity to the access layer as the standard.

The data center network is sized to support the existing applications currently in Tulsa plus the applications that will migrate from Plano. We shall provide the bandwidth required for each migration wave to ensure success.. HPES shall provide the bandwidth required for the Data Center consolidation, using diverse channels on the HPES Global Services Network (GSN) Transport. This is separate from the existing Plano/Tulsa replication circuits, and will therefore have no impact on production replication traffic.

Disaster Recovery. The Tulsa data center will be connected to the Colorado Springs DR site using a dedicated 10GB circuit, providing data replication for DR and off-site backup redundancy.

Once we have tested the new network, we cut over all the current connected equipment, as depicted by the dotted lines in Figure 153. This will be done in a planned change window, but will be transparent to the County because all components are redundant.

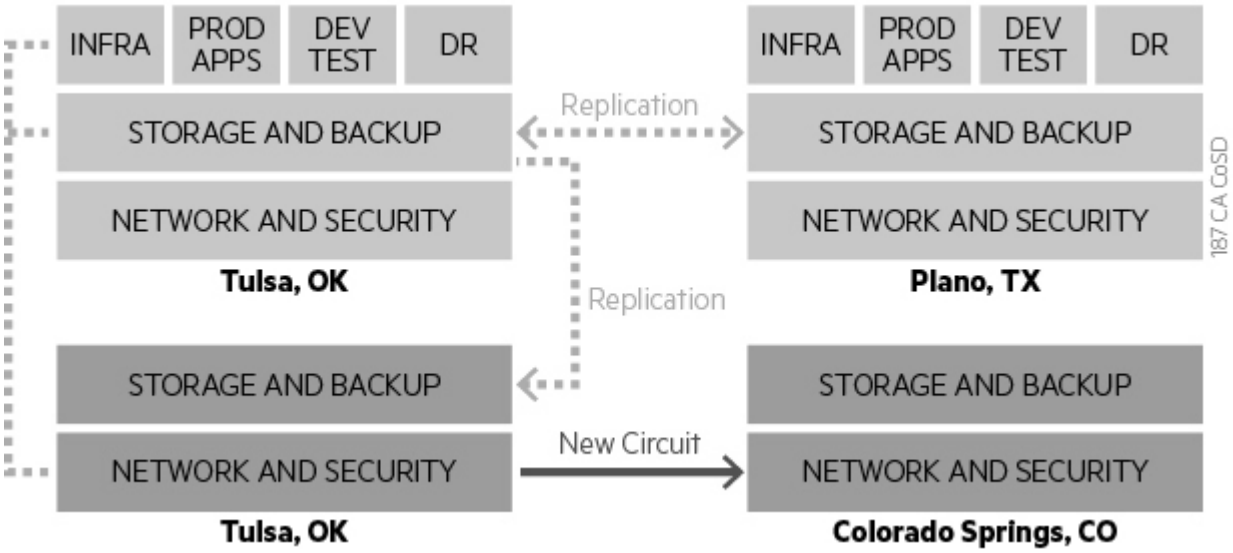
Storage Architecture.

Figure 153below provides a view of the refresh of storage requirements:

Site	Refresh point
Tulsa (SAN, Immutable, VTL)	Transition
Colorado Springs (SAN, Immutable, VTL)	Transition
View Ridge & Lemon Grove (SAN)	Storage Refresh Schedule
AT&T POP (SAN)	Storage Refresh Schedule
DR POP (direct-attached only)	Server Refresh schedule
Rancho Bernardo (SAN, VTL)	Storage Refresh Schedule

The next step is to build out the new storage and backup equipment in both sites, and start synchronizing the data between the current storage array and the new one, as shown in Figure 154. The upgraded storage architecture is fully described in the Storage Architecture Project section, as noted above, which includes a description of the detailed transition activities.

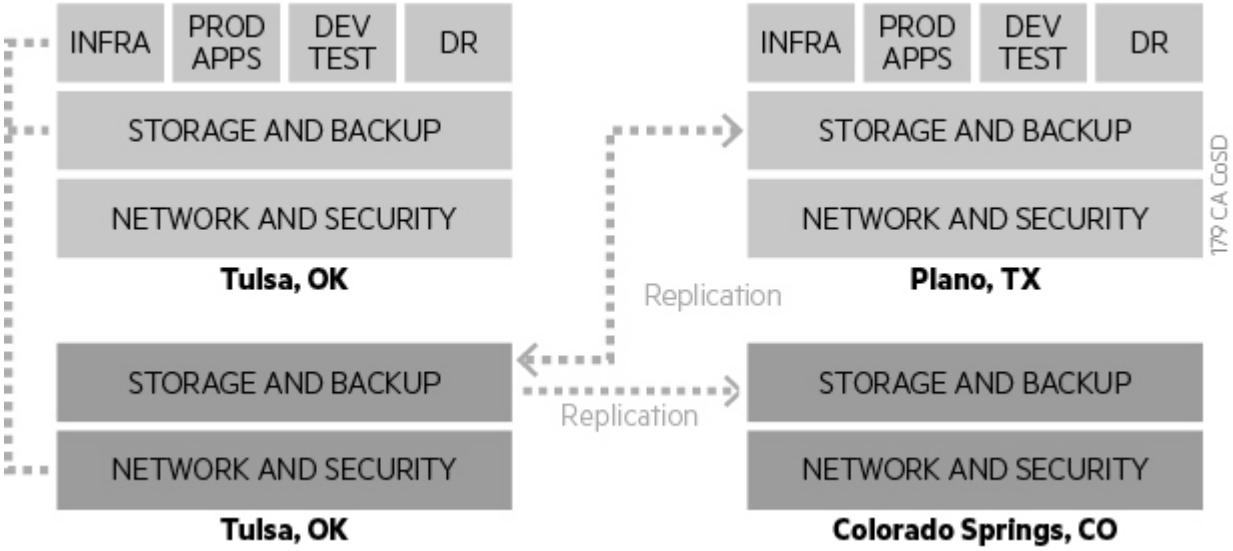
Figure 153. Deploying New Storage, Migrating Data



Once the new storage is fully synchronized with the current production array, we cut over the SAN connectivity (similar approach to the network cutover above, in a planned change window), re-initiate the replication between Tulsa and Plano, and start replicating the DR data to Colorado Springs, as shown in Figure 154

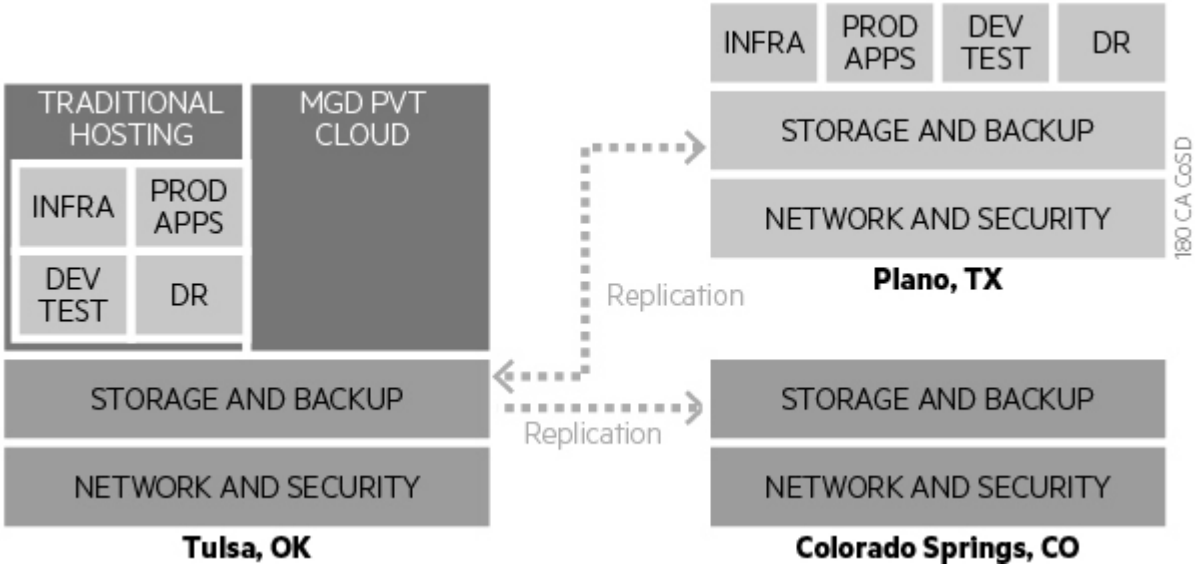
In order to avoid migrating End-Users' Home drive storage twice, the County may wish to migrate this data to OneDrive for Business (ODfB) as defined in the User Data Services Transformation Project prior to the storage migration. HPES shall accommodate this request, provided that the County can commit to supporting HPES in achieving the ODfB migration in 4 months or less from CED (the currently planned schedule calls for 7 months), with larger move groups. If the project cannot be completed in that timeframe, HPES and the County will permit the Data Center consolidation to proceed on schedule anyway (i.e., do not create a dependency between the two projects) in order to avoid the risk that the Data Center Framework Transition will exceed its allowable timeline due to delays in the OneDrive migration.

Figure 154. Cutover to New Storage Arrays



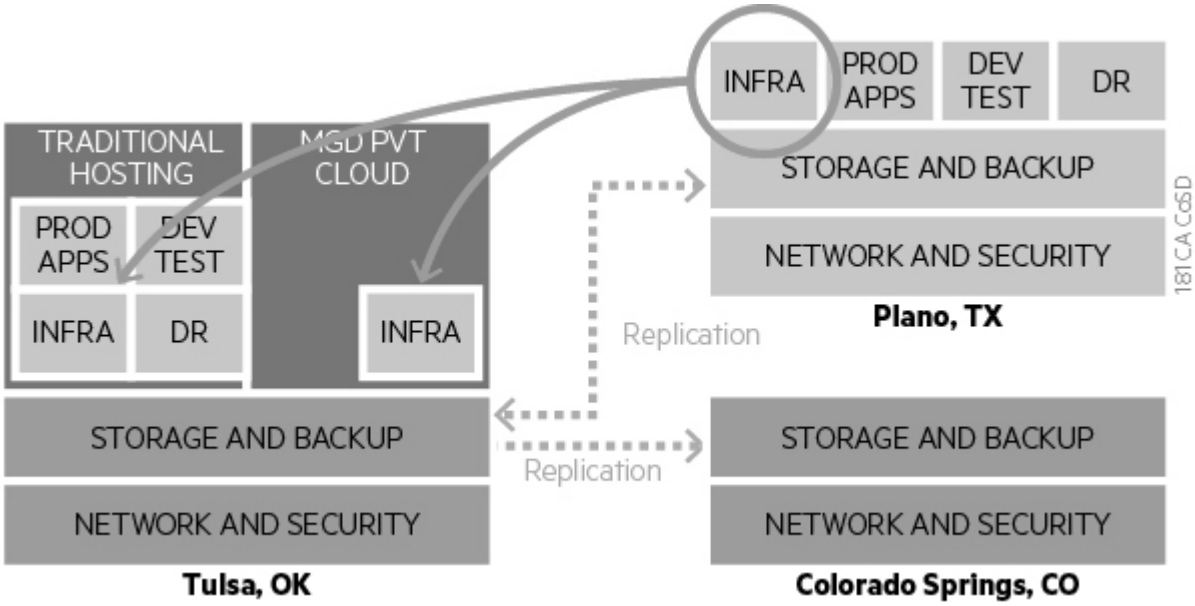
Then we can decommission the old storage and network environments Figure 155. At this point, no migrations have taken place: we have built out the new capacity to support the migration and the hybrid cloud architecture.

Figure 155. Decommission Legacy Network and Storage Hardware in Tulsa



We build out the MPC—your pre-configured cloud resources—while the migration planning and detailed scheduling is taking place Figure 156.

Figure 156. Migration from Plano to Tulsa



HPES – The Expert in Data Center Consolidation

- Unmatched public sector and data center consolidation experience
- Over 150 site consolidations/year using an automated factory approach

Data Center Hybrid Architecture. HPES will deploy hardware and software for a hybrid computing solution that supports applications and infrastructure services for the production and Dev/Test environments. The hybrid architecture combines a HPE Helion Managed Private Cloud (MPC) for cloud-compatible applications and traditional hosting for business applications that are not cloud-compatible, resulting in a hybrid environment. The MPC and the traditional hosted infrastructure are sized to accommodate the combined workloads from Plano and Tulsa, and can scale as needed to support the County's needs.

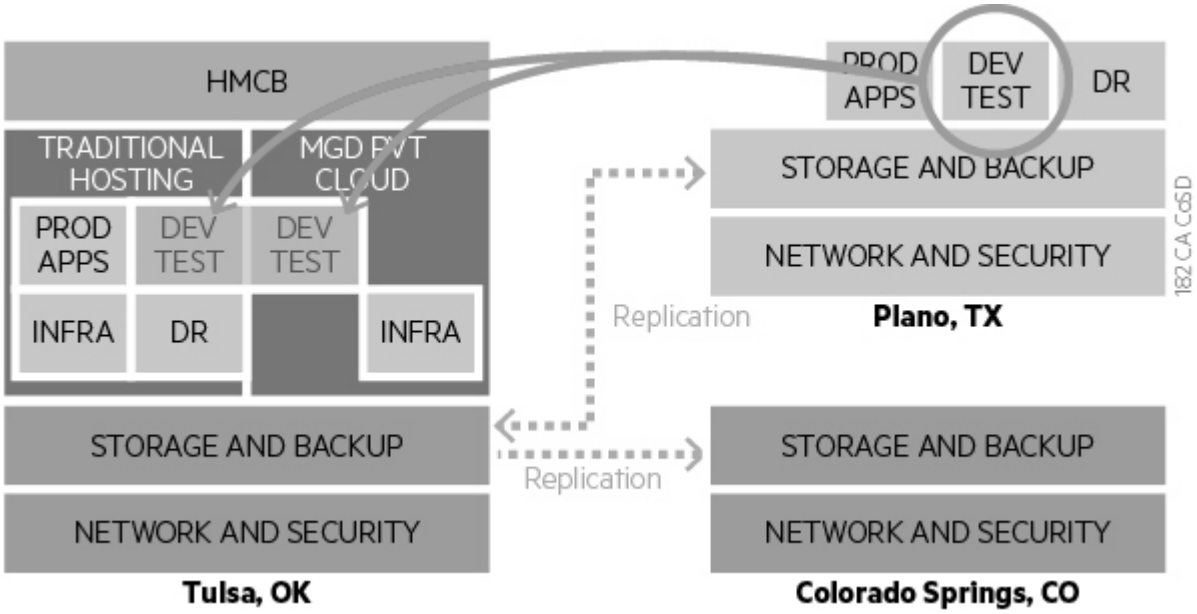
Application servers eligible to be hosted in the MPC include virtual servers that fall into a specific range of sizes, described in detail in Section 2.9,and will run current County approved versions of Windows and Linux.

Servers with resource needs higher than the predefined sizes can be migrated into the largest size, then scaled up to meet their resource needs. Sixty percent of the servers in the data center environment are already located in Tulsa and technically do not have to move to achieve the County's consolidation goal; however, to gain the benefits of automated provisioning and the ability to turn servers up and down for Dev/Test and Applications M&O environments, we have included the cost of moving those that are eligible to be hosted in MPC during the Data Center Transition, to include application regression testing. Sixty-seven percent of the servers in both Plano and Tulsa are eligible to migrate into MPC however, per the County's request, we will not migrate the Tulsa production servers during Transition.

We will work with the application stakeholders' users to identify the best migration windows and methods for each application or related group of applications, and, depending on the platform, we will either migrate them into the Traditional hosting environment or into the MPC, as depicted in Figure 157.

Building out the Cloud Broker will take place in parallel. As we create the pool view of the Dev/Test environment, we will migrate servers from Plano into it, and either keep them live if they are P1/P2 applications or traditional infrastructure, or turn them down if they are P3-P5 in MPC and are not currently being used for a project or active M&O work. See Figure 158.

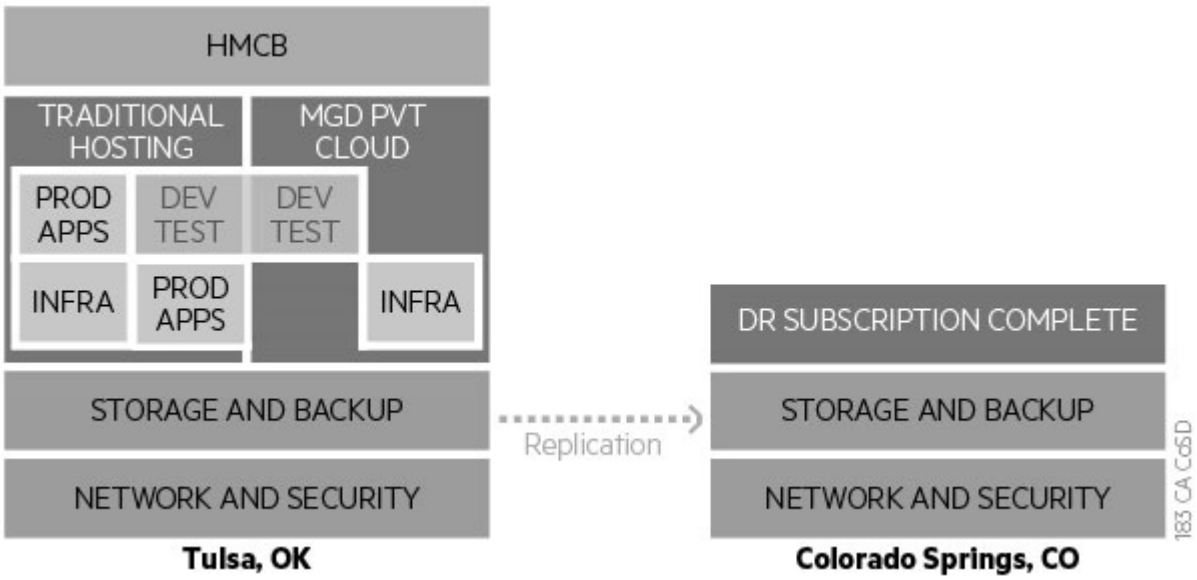
Figure 157. HMCB Deployment, Establishment and Migration into Resource Pools



As we move the production servers, we will make sure that their corresponding DR subscriptions are in place before the migration move group executes. Note that there will be minimal changes to applications—only what is needed to facilitate the migration and redirect any Internet access from using the County's Internet POP to the Leveraged Internet Service.

Once the migration from Plano is complete (or in parallel, as schedules permit), we will move any eligible Test and Development environments in Tulsa into the MPC. As shown in the project schedule, we can complete the build and the migration in as little as 7 months or we can move at a longer cadence if the business dictates. The County's required Transition period allows for two additional months to complete the project. The migration plan and pricing include moving any eligible Tulsa server environments into the MPC; however, these moves can be deferred to the refresh timeframe, if this is the County's preference.

Figure 158. Future Mode of Operations



Note that the mainframe and AS400 environments will need to remain intact beyond the end of the Transition period. The infrastructure required to support those environments will remain in Plano for as long as those systems are needed.

E-mail. The E-Mail transition is fully described in the Email Transition Project section and includes a description of the detailed transition activities.

Rationale

The hybrid environment designed for the Tulsa data center brings to the County key application infrastructure improvements throughout the life cycle of an application, whether it is in MPC or the traditional environment, and whether it resides on a physical server or a virtual host. Our complete hybrid cloud solution will bring to bear streamlined service creation, deployment, and monitoring for application workloads throughout the data center. We will enable multivendor support across hypervisors, OS instances, and infrastructure. The private cloud environment we propose consists of server, storage, and networking built for the cloud. It also consists of security, automation, and management software designed for hybrid delivery. The standardization, automation, and converged building blocks of our solution will allow the County to respond to changing business needs faster by deploying timely resources

where needed most, and in the most cost-efficient manner. Our solution is designed to enable the County to meet performance, availability, security and compliance requirements.

Based on the single data center requirement in the RFP, we have proposed consolidating the data center workload that is currently hosted in the HPES Plano, Texas data center facility into our Tulsa, Oklahoma facility.

The inclusion of the Cloud Broker solution in our proposal is based on the County's desire to have hybrid cloud capabilities in the future. Our Cloud Broker solution will provide the County with an enterprise view of all data center platforms, including private cloud, public cloud, and traditional hosting environments. The cloud broker will give the County the ability to have an enterprise view of system performance as well as financial management across each of the hybrid platform through one pane of glass. It also will provide a single console for provisioning compute resources across the County's hybrid estate.

We are proposing a MPC solution for part of the workload that can be easily ported to a cloud to provide a highly virtualized environment with automation that will reduce costs to the County.

The following Table **73** lists all requirements defined in RFP Exhibit H, Schedule 4.3 that helped us craft the solutions that best met the requirements as we understood them.

Table 73**. Exhibit H, Schedule 4.3**

RFP EXHIBIT	PAGE	HPES SOLUTION	REQUIREMENT
Exhibit H, 4.3 Operations Services	p215	Cloud Broker	The data center must be capable of providing hybrid services to County approved cloud based applications and services
Exhibit H, 4.3 Operations Services	p215	Managed Private Cloud	The data center must be capable of providing hybrid services to County approved cloud based applications and services, be a highly virtualized environment with respect to network, storage and servers and must maintain its own installed and secure Internet connection.
Exhibit H, 4.3 Operations Services	p219, Item 29	Data Center Consolidation	Develop a single data center operations.
Exhibit H, 4.3 Operations Services	P216, section 6.2.1.2	Cloud Broker	Contractor shall perform centralized management and performance monitoring of Data Center Services.
Exhibit H, 4.3 Operations Services	P220, Item 31	Managed Private Cloud	Develop a secure flexible Services model when and where appropriate so that the County shall have the flexibility to quickly grow or reduce consumption.
Exhibit H, 4.3	P230, Section 6.7.2.14	Managed Private Cloud	Contractor shall continuously improve and reduce costs with integrated tools that provide better security and control of the Application infrastructure.

RFP EXHIBIT	PAGE	HPES SOLUTION	REQUIREMENT
Operations Services			
Exhibit H, 4.3 Operations Services	P230, Section 6.7.2.16	Managed Private Cloud	Contractor shall continuously improve speed of delivery for new Applications and Services in Application infrastructure.
Exhibit H, 4.3 Operations Services	P230, Section 6.7.2.21	Managed Private Cloud	Contractor shall maintain Application Infrastructure Services so there is not a single point failure thereby assuring County business applications continue to operate during any unplanned event.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES will assign a data center consolidation transition project manager (TPM) that will report to the Transition Services Manager. The TPM will have overall responsibility for this project and will be the primary point of contact for the County in support of all data center consolidation activities. This TPM will be responsible for maintaining the HPES Move Group Plan and collaborating with the County's designated project leader, as well as coordinating activities with the other TPMs and the HPES Project Management Office. Knowing the importance of this initiative to the County, we have also identified an HPES account executive sponsor to provide executive visibility throughout the project.

The data center consolidation TPM will be directly responsible for all activities associated with the DR and storage architecture subproject activities and provide oversight of the team. The TPM will be assisted by:

- Another TPM that will be responsible for the buildout and testing of the cloud components
- A TPM whose focus is applications readiness, and will work closely with the County and the HPES team to closely manage application testing, remediation (if necessary), and scheduling priorities of the County stakeholders.

Our virtual support includes architects, engineers, and migration specialists with specialized expertise in each of the disciplines required to deliver the various components of the plan. Additional details on overall transition staffing are provided in Section 2.11, Requirements, in response to Schedule 2.1, Section 2.

The data center facilities at Tulsa, Plano, and Colorado Springs are required to support transition. The transition project management teams will be headquartered at our Rancho Bernardo facility.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

Transition Schedule and Tasks

As described above, HPES will use a phased transition approach to accomplish the data center transition. For each phase, we will follow a standard process that includes an assessment of the existing environment to adjust for any changes that have occurred between the time we developed the solution and the effective date, and the status of any in-flight projects. This information will help us finalize our transition plan activities, timing, and dependencies. As we begin the design process, we seek to optimize network connections, server configurations, and storage platforms to improve speed, and take advantage of higher

capacity hardware that is faster and more efficient to deliver a lower cost solution. Each phase of the plan includes submission of project deliverables to the County for review, response, and subsequent approval, and all approved project deliverables will be made available to authorized users via the Service Portal.

The high-level planning activities for the data center consolidation are summarized in Figure 159**.** Because the data center transition has a number of interdependencies and subprojects, we will first initiate a planning and governance phase, as part of the overall transition high-level planning sessions, which will kick off this set of projects.

Consolidation Assessment. In preparation for the migration of the applications from Plano, we will assess the current Dev/Test and production environments to classify servers in terms of their migration targets and analyze server mapping. The results of the assessment will help us to develop the plan for migrating the applications, data, and infrastructure. This process is described further below.

Following the high-level planning activity, we will move directly into the detailed design and build phases. The first part of the implementation is the data center network. The draft data center network transition plan is depicted in Figure 160. An early output from the assessment will be identification/verification of additional network bandwidth needed in the Tulsa data center. We use this information to engineer the new network design and identify the specific network devices and configurations to be ordered and installed in Tulsa. We will submit this plan to the County for approval prior to placing equipment orders. Once approved, we will develop the final Bill of Materials and order the equipment.

With receipt of the equipment, HPES will begin installation of the data center network compartments in both Tulsa and Colorado Springs. In the Tulsa environment, we will create interconnects between the existing and new network infrastructure, then reroute traffic to the new or upgraded circuits. An integral part of the new network architecture is the establishment of the firewalls/IPS' and security zones needed to support traffic segregation and authorized third-party access. As part of the overall testing process, we will validate and test third-party access to the new network environment. Once testing is successful, we will move the network design deliverables to "as-built" documents, update all process documentation based on the new technologies, and submit all required deliverables to the County for review and approval.

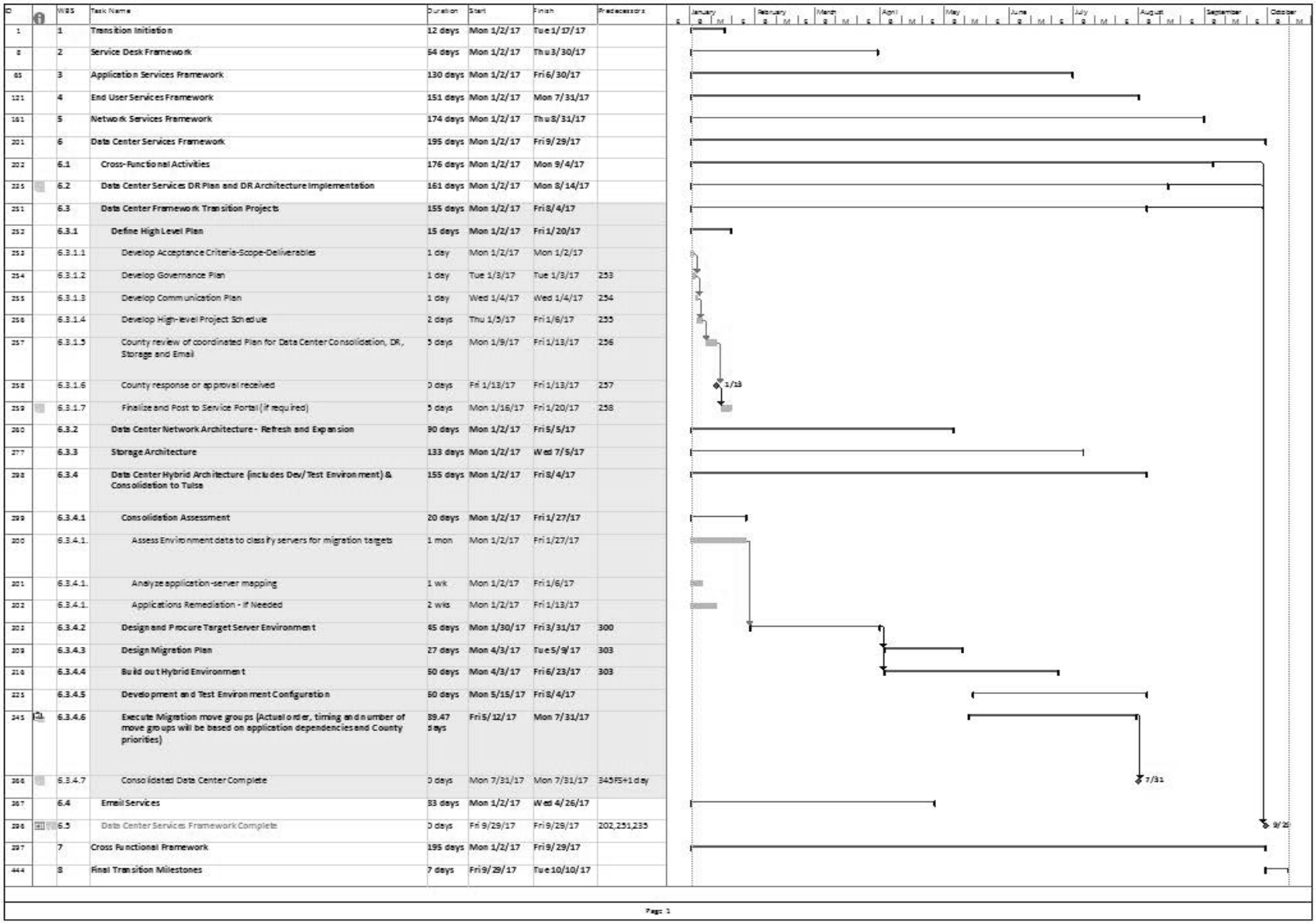
As the network design and buildout is taking place, we will also be analyzing the DR requirements. The draft DR transition plan activities are shown in Figure 161.

As part of the Data Center Consolidation transition design process, HPES will seek to optimize County software licensing costs. Existing County software has a variety of licensing models such as site/enterprise, concurrent user, named user, module, managed budget, server, CPU, and core. Licenses based on server, CPU, and core present an opportunity for consolidation and license cost savings. Examples of County vendors that use these types of licensing models for enterprise server software include Adobe, EMC, Microsoft, Oracle, Symantec, IBM, and VMware.

Methodologies to reduce license obligations for server/CPU/core based licenses include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated to headroom at each site versus single site's shared environment.

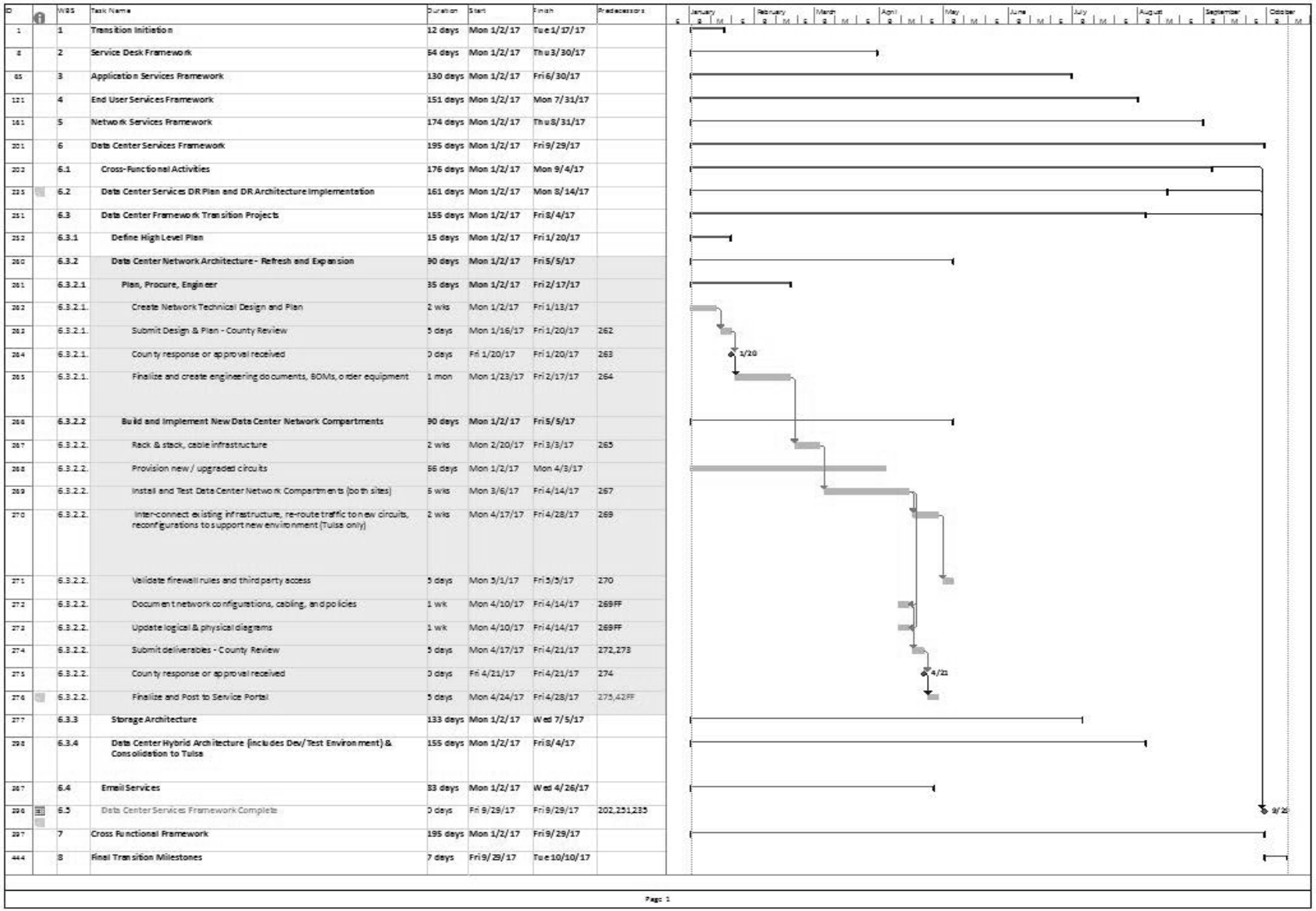
MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases.

Figure 159. Data Center Consolidation Planning and Assessment



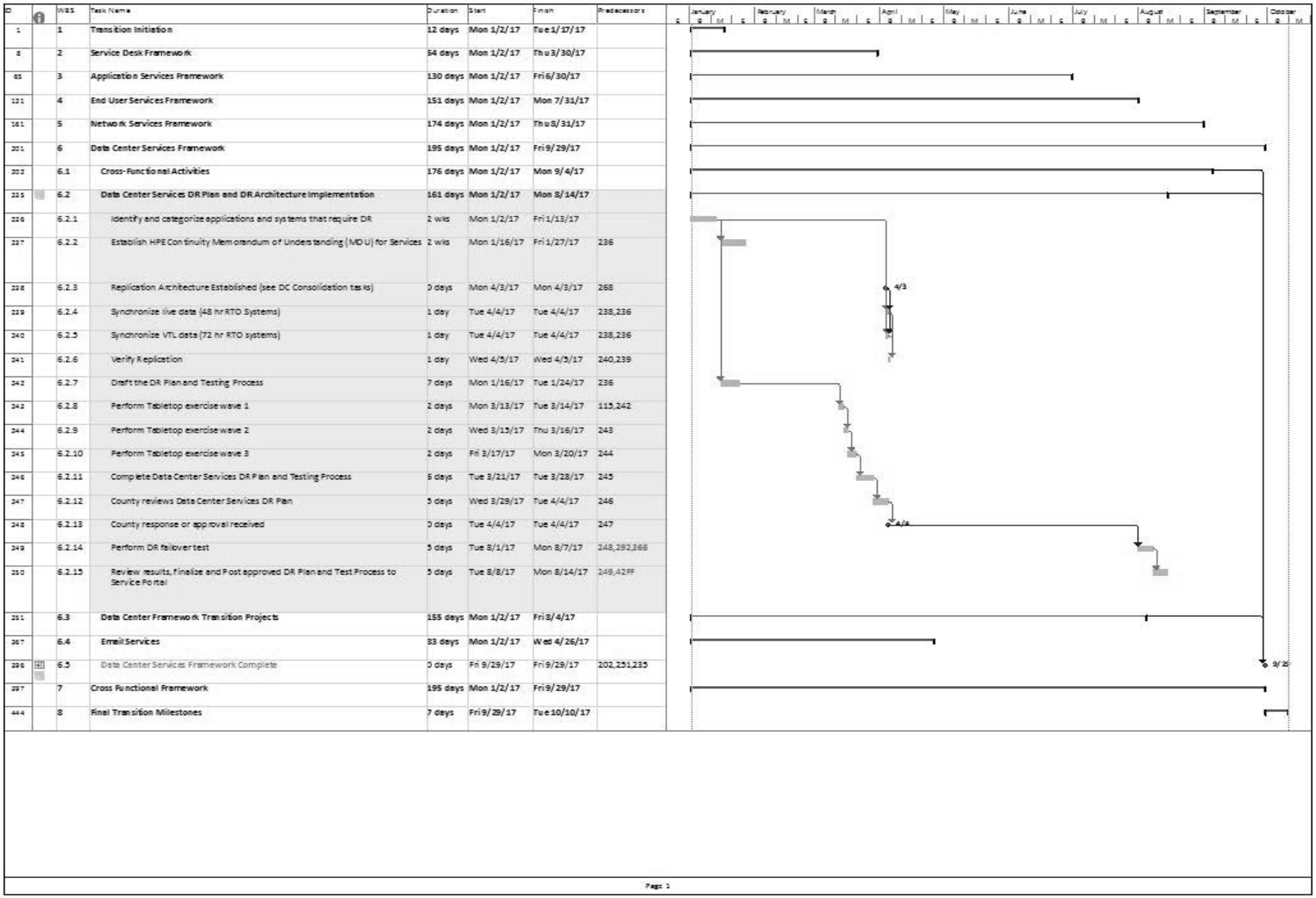
ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
225	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
252	6.3.1	Define High Level Plan	15 days	Mon 1/2/17	Fri 1/20/17	
253	6.3.1.1	Develop Acceptance Criteria-Scope-Deliverables	1 day	Mon 1/2/17	Mon 1/2/17	
254	6.3.1.2	Develop Governance Plan	1 day	Tue 1/3/17	Tue 1/3/17	253
255	6.3.1.3	Develop Communication Plan	1 day	Wed 1/4/17	Wed 1/4/17	254
256	6.3.1.4	Develop High-level Project Schedule	2 days	Thu 1/5/17	Fri 1/6/17	255
257	6.3.1.5	County review of coordinated Plan for Data Center Consolidation, DR, Storage and Email	5 days	Mon 1/9/17	Fri 1/13/17	256
258	6.3.1.6	County response or approval received	0 days	Fri 1/13/17	Fri 1/13/17	257
259	6.3.1.7	Finalize and Post to Service Portal (if required)	5 days	Mon 1/16/17	Fri 1/20/17	258
260	6.3.2	Data Center Network Architecture - Refresh and Expansion	90 days	Mon 1/2/17	Fri 5/5/17	
277	6.3.3	Storage Architecture	133 days	Mon 1/2/17	Wed 7/5/17	
298	6.3.4	Data Center Hybrid Architecture (includes Dev/Test Environment) & Consolidation to Tulsa	155 days	Mon 1/2/17	Fri 8/4/17	
299	6.3.4.1	Consolidation Assessment	20 days	Mon 1/2/17	Fri 1/27/17	
200	6.3.4.1.	Assess Environment data to classify servers for migration targets	1 mon	Mon 1/2/17	Fri 1/27/17	
201	6.3.4.1.	Analyze application-server mapping	1 wk	Mon 1/2/17	Fri 1/6/17	
202	6.3.4.1.	Applications Remediation - if Needed	2 wks	Mon 1/2/17	Fri 1/13/17	
203	6.3.4.2	Design and Procure Target Server Environment	45 days	Mon 1/30/17	Fri 3/31/17	300
209	6.3.4.3	Design Migration Plan	27 days	Mon 4/3/17	Tue 5/9/17	303
216	6.3.4.4	Build out Hybrid Environment	50 days	Mon 4/3/17	Fri 6/23/17	303
225	6.3.4.5	Development and Test Environment Configuration	60 days	Mon 5/15/17	Fri 8/4/17	
245	6.3.4.6	Execute Migration move groups (Actual order, timing and number of move groups will be based on application dependencies and County priorities)	39.47 days	Fri 5/12/17	Mon 7/31/17	
266	6.3.4.7	Consolidated Data Center Complete	0 days	Mon 7/31/17	Mon 7/31/17	345FS+1 day
267	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17	
296	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
297	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

Figure 160. Data Center Network Transition Activities



ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
215	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
252	6.3.1	Define High Level Plan	15 days	Mon 1/2/17	Fri 1/20/17	
260	6.3.2	Data Center Network Architecture - Refresh and Expansion	90 days	Mon 1/2/17	Fri 5/5/17	
261	6.3.2.1	Plan, Procure, Engineer	35 days	Mon 1/2/17	Fri 2/17/17	
262	6.3.2.1.	Create Network Technical Design and Plan	2 wks	Mon 1/2/17	Fri 1/13/17	
263	6.3.2.1.	Submit Design & Plan - County Review	5 days	Mon 1/16/17	Fri 1/20/17	262
264	6.3.2.1.	County response or approval received	0 days	Fri 1/20/17	Fri 1/20/17	263
265	6.3.2.1.	Finalize and create engineering documents, BOMs, order equipment	1 mon	Mon 1/23/17	Fri 2/17/17	264
266	6.3.2.2	Build and Implement New Data Center Network Compartments	90 days	Mon 1/2/17	Fri 5/5/17	
267	6.3.2.2.	Rack & stack, cable infrastructure	2 wks	Mon 2/20/17	Fri 3/3/17	265
268	6.3.2.2.	Provision new / upgraded circuits	66 days	Mon 1/2/17	Mon 4/3/17	
269	6.3.2.2.	Install and Test Data Center Network Compartments (both sites)	5 wks	Mon 3/6/17	Fri 4/14/17	267
270	6.3.2.2.	Inter-connect existing infrastructure, re-route traffic to new circuits, reconfigurations to support new environment (Tulsa only)	2 wks	Mon 4/17/17	Fri 4/28/17	269
271	6.3.2.2.	Validate firewall rules and third party access	5 days	Mon 5/1/17	Fri 5/5/17	270
272	6.3.2.2.	Document network configurations, cabling, and policies	1 wk	Mon 4/10/17	Fri 4/14/17	269FF
273	6.3.2.2.	Update logical & physical diagrams	1 wk	Mon 4/10/17	Fri 4/14/17	269FF
274	6.3.2.2.	Submit deliverables - County Review	5 days	Mon 4/17/17	Fri 4/21/17	272,273
275	6.3.2.2.	County response or approval received	0 days	Fri 4/21/17	Fri 4/21/17	274
276	6.3.2.2.	Finalize and Post to Service Portal	5 days	Mon 4/24/17	Fri 4/28/17	275,42FF
277	6.3.3	Storage Architecture	133 days	Mon 1/2/17	Wed 7/5/17	
293	6.3.4	Data Center Hybrid Architecture (includes Dev/Test Environment) & Consolidation to Tulsa	155 days	Mon 1/2/17	Fri 8/4/17	
297	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17	
296	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
297	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

Figure 161. Data Center DR Transition Activities



ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	54 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
225	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
226	6.2.1	Identify and categorize applications and systems that require DR	2 wks	Mon 1/2/17	Fri 1/13/17	
227	6.2.2	Establish HPE Continuity Memorandum of Understanding (MOU) for Services	2 wks	Mon 1/16/17	Fri 1/27/17	226
228	6.2.3	Replication Architecture Established (see DC Consolidation tasks)	0 days	Mon 4/3/17	Mon 4/3/17	268
229	6.2.4	Synchronize live data (48 hr RTO Systems)	1 day	Tue 4/4/17	Tue 4/4/17	238,236
240	6.2.5	Synchronize VTL data (72 hr RTO systems)	1 day	Tue 4/4/17	Tue 4/4/17	238,236
241	6.2.6	Verify Replication	1 day	Wed 4/5/17	Wed 4/5/17	240,239
242	6.2.7	Draft the DR Plan and Testing Process	7 days	Mon 1/16/17	Tue 1/24/17	236
243	6.2.8	Perform Tabletop exercise wave 1	2 days	Mon 3/13/17	Tue 3/14/17	115,242
244	6.2.9	Perform Tabletop exercise wave 2	2 days	Wed 3/15/17	Thu 3/16/17	243
245	6.2.10	Perform Tabletop exercise wave 3	2 days	Fri 3/17/17	Mon 3/20/17	244
246	6.2.11	Complete Data Center Services DR Plan and Testing Process	5 days	Tue 3/21/17	Tue 3/28/17	245
247	6.2.12	County reviews Data Center Services DR Plan	5 days	Wed 3/29/17	Tue 4/4/17	246
248	6.2.13	County response or approval received	0 days	Tue 4/4/17	Tue 4/4/17	247
249	6.2.14	Perform DR failover test	5 days	Tue 8/1/17	Mon 8/7/17	248,282,366
250	6.2.15	Review results, finalize and Post approved DR Plan and Test Process to Service Portal	5 days	Tue 8/8/17	Mon 8/14/17	248,42FF
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
267	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17	
296	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
297	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

Data Center Services DR Plan and DR Architecture Implementation. As part of the consolidation analysis, we will review the applications' DR requirements to adjust the current solution for any changes to applications' configuration or DR requirements, and provide updated specifications to the HPES continuity team. Any buildout of the subscription-based service environment that might be needed is triggered by our internal notification and agreements for the DR relationship, and does not require transition resources assigned to this project to coordinate or procure equipment, beyond the dedicated network elements. The HPES continuity team is aware of the County's requirements, based on the solution we are proposing, and will be updated upon notification of award so that any prework needed to prepare the DR environment will be completed in time for the new contract. The other dedicated component of the DR environment, the refreshed Centera, is discussed in the Storage Architecture project (response to Schedule 2.1, Section 3.5).

Once the network connectivity between the Tulsa and Colorado Springs is established, we will begin replicating both live data and virtual tape library (VTL) data and verify that data replication is occurring accurately and as planned. At the end of the phase, HPES will perform three tabletop exercises of the DR plan to validate its functionality and address any deficiencies found during the exercise. Following successful completion of these exercises, at least 90 days prior to the cutover date for the data center framework, HPES will submit the draft DR plan for framework to the County for review and comment. Once we have at least a few applications running in the Tulsa environment, we will schedule an actual failover test. Note that using the HPE Helion team's established DR testing methods, a failover test can be accomplished without forcing an actual outage to the production applications.

Figure 162 provides a summary of activities in our draft transition plan for building out the Tulsa data center target environment.

Data Center Hybrid Architecture and Consolidation to Tulsa

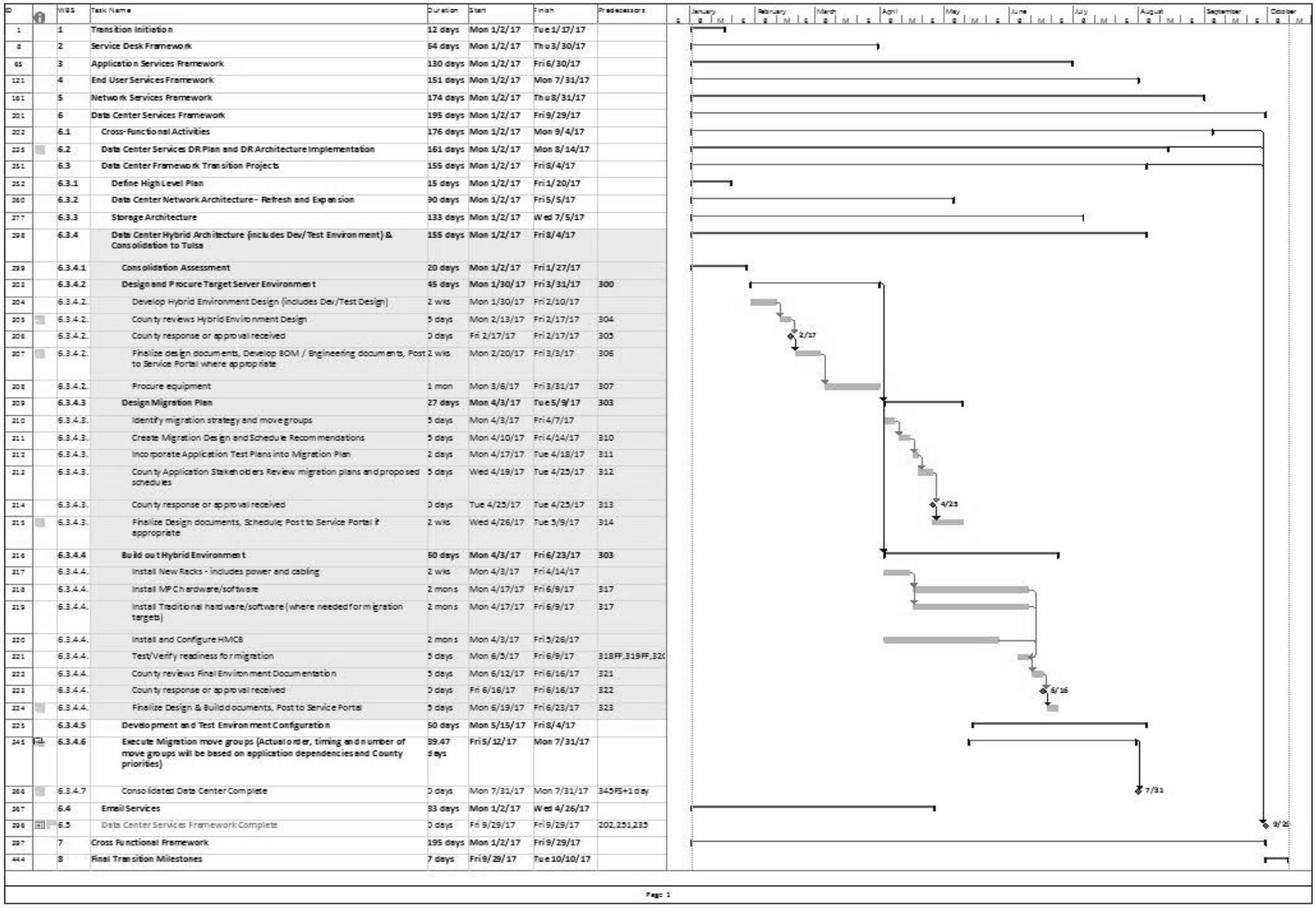
Consolidation Assessment. As described above, we will assess the Plano application and infrastructure environment to identify the migration approach for each. We will prepare a source-to-target mapping that documents each of the servers that will be migrated along with the target server characteristics during this stage. We will also do an assessment of application requirements to the services provided by the MPC to determine compatibility. If there is a match, the application's Dev/Test and/or Break/Fix servers will be moved into MPC. HPES will work collaboratively with the County's business users to determine the most appropriate solution for each application. Our applications team will review the applications targeted to migrate to verify if they have any common issues that need to be mitigated prior to migration, such as hard-coded IP addresses. If we discover any issues, we will mitigate them prior to migration, using established change control procedures. From this process, we will have a clear picture of where we will need new equipment and where we will have opportunities for reuse and for migration using a pack-and-ship approach, and can refine and adjust the target server environment solution (developed for this proposal) into a design that reflects the detailed configurations including any changes that have occurred since submission.

Design and Procure Target Server Environment. We will design the hybrid environment in Tulsa to include:

- MPC and Cloud Broker (HMCB)
- Expansion of the capacity of the existing traditional infrastructure in Tulsa to accommodate workloads from Plano that require traditional hosting.

From the completed design documents, we will develop Bills of Materials and engineering documents, and submit internal purchase orders for any new hardware and software required. There is no additional cost beyond the Transition price for this activity.

Figure 162. Notional Transition Plan for Data Center Build-out and Consolidation Design



ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
225	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
252	6.3.1	Define High Level Plan	15 days	Mon 1/2/17	Fri 1/20/17	
260	6.3.2	Data Center Network Architecture - Refresh and Expansion	90 days	Mon 1/2/17	Fri 5/5/17	
277	6.3.3	Storage Architecture	133 days	Mon 1/2/17	Wed 7/5/17	
298	6.3.4	Data Center Hybrid Architecture (includes Dev/Test Environment) & Consolidation to Tulsa	155 days	Mon 1/2/17	Fri 8/4/17	
299	6.3.4.1	Consolidation Assessment	20 days	Mon 1/2/17	Fri 1/27/17	
303	6.3.4.2	Design and Procure Target Server Environment	45 days	Mon 1/30/17	Fri 3/31/17	300
304	6.3.4.2.	Develop Hybrid Environment Design (includes Dev/Test Design)	2 wks	Mon 1/30/17	Fri 2/10/17	
305	6.3.4.2.	County reviews Hybrid Environment Design	5 days	Mon 2/13/17	Fri 2/17/17	304
306	6.3.4.2.	County response or approval received	0 days	Fri 2/17/17	Fri 2/17/17	305
307	6.3.4.2.	Finalize design documents, Develop BOM / Engineering documents, Post to Service Portal where appropriate	2 wks	Mon 2/20/17	Fri 3/3/17	306
308	6.3.4.2.	Procure equipment	1 mon	Mon 3/6/17	Fri 3/31/17	307
309	6.3.4.3	Design Migration Plan	27 days	Mon 4/3/17	Tue 5/9/17	303
310	6.3.4.3.	Identify migration strategy and move groups	5 days	Mon 4/3/17	Fri 4/7/17	
311	6.3.4.3.	Create Migration Design and Schedule Recommendations	5 days	Mon 4/10/17	Fri 4/14/17	310
312	6.3.4.3.	Incorporate Application Test Plans into Migration Plan	2 days	Mon 4/17/17	Tue 4/18/17	311
313	6.3.4.3.	County Application Stakeholders Review migration plans and proposed schedules	5 days	Wed 4/19/17	Tue 4/25/17	312
314	6.3.4.3.	County response or approval received	0 days	Tue 4/25/17	Tue 4/25/17	313
315	6.3.4.3.	Finalize Design documents, Schedule; Post to Service Portal if appropriate	2 wks	Wed 4/26/17	Tue 5/9/17	314
316	6.3.4.4	Build out Hybrid Environment	60 days	Mon 4/3/17	Fri 6/23/17	303
317	6.3.4.4.	Install New Racks - includes power and cabling	2 wks	Mon 4/3/17	Fri 4/14/17	
318	6.3.4.4.	Install MPC hardware/software	2 mons	Mon 4/17/17	Fri 6/9/17	317
319	6.3.4.4.	Install Traditional hardware/software (where needed for migration targets)	2 mons	Mon 4/17/17	Fri 6/9/17	317
320	6.3.4.4.	Install and Configure HMC8	2 mons	Mon 4/3/17	Fri 5/26/17	
321	6.3.4.4.	Test/Verify readiness for migration	5 days	Mon 6/5/17	Fri 6/9/17	318FF,319FF,32(
322	6.3.4.4.	County reviews Final Environment Documentation	5 days	Mon 6/12/17	Fri 6/16/17	321
323	6.3.4.4.	County response or approval received	0 days	Fri 6/16/17	Fri 6/16/17	322
324	6.3.4.4.	Finalize Design & Build documents, Post to Service Portal	5 days	Mon 6/19/17	Fri 6/23/17	323
325	6.3.4.5	Development and Test Environment Configuration	50 days	Mon 5/15/17	Fri 8/4/17	
345	6.3.4.6	Execute Migration move groups (Actual order, timing and number of move groups will be based on application dependencies and County priorities)	89.47 days	Fri 5/12/17	Mon 7/31/17	
366	6.3.4.7	Consolidated Data Center Complete	0 days	Mon 7/31/17	Mon 7/31/17	345FS+1 day
367	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17	
396	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
397	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

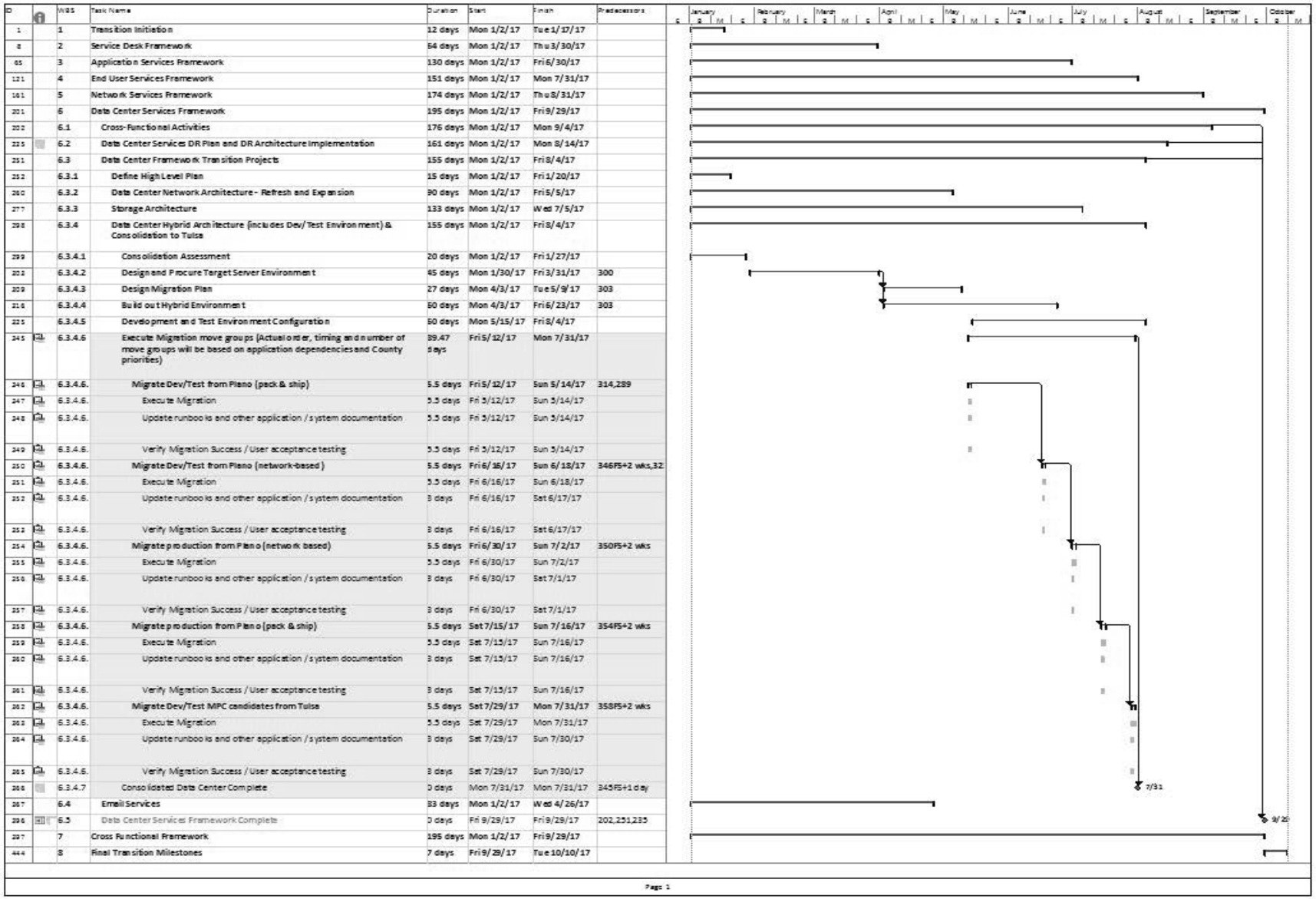
Design Migration Plan. During the design phase we also identify move groups that will organize the servers according to application dependencies, and incorporate other critical factors such as the change "freeze" periods, allowable maintenance windows, and other business priorities. The intent is to migrate all applications supporting a business process together when possible rather than migrating individual applications, reducing risk to the County business processes. In addition, this will assist in the County's understanding of the order in which the detailed design and migrations should take place and enable the project to complete in the proposed time frame. We will assign a work packet for each server group supporting the same application, which are combined into move groups based on the critical factors identified above and application resource availability. We will create a consolidated move group plan that we will present to the County for approval.

Build-Out Hybrid Environment. The build-out of the hybrid environment includes installing new racks, power and cabling, installing, and configuring the MPC and traditional hardware and software. We will also install and configure the HMCB. We will perform tests on the newly built servers to verify that automation processes as well as traditional connectivity and configurations to existing back-end management and reporting systems are in place, then create or update documentation for the target systems. Note that the storage architecture will have been built out under a separate but integrated plan: at this point in time, the two schedules converge. Once the build is complete and tested, we are ready to begin migrating move groups over the network. Tasks to build out the Dev/Test environment capabilities will also commence during this phase. These activities are described in the response to Development and Test Environment, Schedule 2.1, Section 3.3.

During this time, HPES will work with County application stakeholders to create the detailed Migration Runbook and other subdeliverables, such as the Back Out plan, and determine the change window to execute the go-live. During this phase, we will work with and provide guidance to the County to plan the tasks and secure required resources to successfully execute the Migration Runbook Plan. We will also begin the necessary change management steps and communications processes in conjunction with the County.

Figure 163 shows the types of migrations we may perform, for illustration only. The actual number, types, and scheduling of move groups will be established in coordination with County stakeholders. In the illustration, weekend dates are used, to illustrate off-hours activity, such as for pack-and-ship migrations; however actual scheduling and the full set of tasks will be solidified during the migration planning.

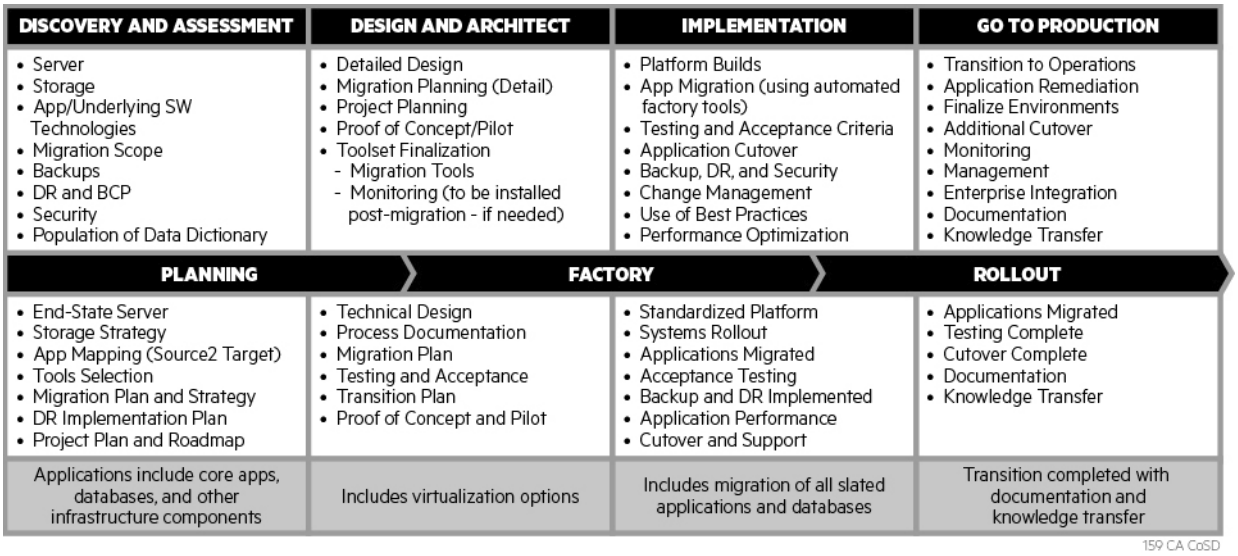
Figure 163. Draft Migration Plan Activities



ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
225	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
252	6.3.1	Define High Level Plan	15 days	Mon 1/2/17	Fri 1/20/17	
260	6.3.2	Data Center Network Architecture - Refresh and Expansion	90 days	Mon 1/2/17	Fri 5/5/17	
277	6.3.3	Storage Architecture	133 days	Mon 1/2/17	Wed 7/5/17	
298	6.3.4	Data Center Hybrid Architecture (includes Dev/Test Environment) & Consolidation to Tulsa	155 days	Mon 1/2/17	Fri 8/4/17	
299	6.3.4.1	Consolidation Assessment	20 days	Mon 1/2/17	Fri 1/27/17	
303	6.3.4.2	Design and Procure Target Server Environment	45 days	Mon 1/30/17	Fri 3/31/17	300
309	6.3.4.3	Design Migration Plan	27 days	Mon 4/3/17	Tue 5/9/17	303
316	6.3.4.4	Build out Hybrid Environment	60 days	Mon 4/3/17	Fri 6/23/17	303
325	6.3.4.5	Development and Test Environment Configuration	60 days	Mon 5/15/17	Fri 8/4/17	
345	6.3.4.6	Execute Migration move groups (Actual order, timing and number of move groups will be based on application dependencies and County priorities)	39.47 days	Fri 5/12/17	Mon 7/31/17	
346	6.3.4.6.	Migrate Dev/Test from Plano (pack & ship)	5.5 days	Fri 5/12/17	Sun 5/14/17	314,289
347	6.3.4.6.	Execute Migration	5.5 days	Fri 5/12/17	Sun 5/14/17	
348	6.3.4.6.	Update runbooks and other application / system documentation	5.5 days	Fri 5/12/17	Sun 5/14/17	
349	6.3.4.6.	Verify Migration Success / User acceptance testing	5.5 days	Fri 5/12/17	Sun 5/14/17	
350	6.3.4.6.	Migrate Dev/Test from Plano (network-based)	5.5 days	Fri 6/16/17	Sun 6/18/17	346FS+2 wks,32
351	6.3.4.6.	Execute Migration	5.5 days	Fri 6/16/17	Sun 6/18/17	
352	6.3.4.6.	Update runbooks and other application / system documentation	3 days	Fri 6/16/17	Sat 6/17/17	
353	6.3.4.6.	Verify Migration Success / User acceptance testing	3 days	Fri 6/16/17	Sat 6/17/17	
354	6.3.4.6.	Migrate production from Plano (network based)	5.5 days	Fri 6/30/17	Sun 7/2/17	350FS+2 wks
355	6.3.4.6.	Execute Migration	5.5 days	Fri 6/30/17	Sun 7/2/17	
356	6.3.4.6.	Update runbooks and other application / system documentation	3 days	Fri 6/30/17	Sat 7/1/17	
357	6.3.4.6.	Verify Migration Success / User acceptance testing	3 days	Fri 6/30/17	Sat 7/1/17	
358	6.3.4.6.	Migrate production from Plano (pack & ship)	5.5 days	Sat 7/15/17	Sun 7/16/17	354FS+2 wks
359	6.3.4.6.	Execute Migration	5.5 days	Sat 7/15/17	Sun 7/16/17	
360	6.3.4.6.	Update runbooks and other application / system documentation	3 days	Sat 7/15/17	Sun 7/16/17	
361	6.3.4.6.	Verify Migration Success / User acceptance testing	3 days	Sat 7/15/17	Sun 7/16/17	
362	6.3.4.6.	Migrate Dev/Test MPC candidates from Tulsa	5.5 days	Sat 7/29/17	Mon 7/31/17	358FS+2 wks
363	6.3.4.6.	Execute Migration	5.5 days	Sat 7/29/17	Mon 7/31/17	
364	6.3.4.6.	Update runbooks and other application / system documentation	3 days	Sat 7/29/17	Sun 7/30/17	
365	6.3.4.6.	Verify Migration Success / User acceptance testing	3 days	Sat 7/29/17	Sun 7/30/17	
366	6.3.4.7	Consolidated Data Center Complete	0 days	Mon 7/31/17	Mon 7/31/17	345FS+1 day
367	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17	
396	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
397	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

Execute Migration Move Groups. The HPES Migration Factory embodies a proven methodology and phases as well as best practices that HPES uses on all of our data center consolidation projects. An overview of the phases is provided in Figure 164.

Figure 164. Migration Factory Methodology



Adherence to this methodology enables HPES to deliver a flawless data center consolidation.

During the assessment and design phases of the project, we will build a migration roadmap detailing the placement, design, and execution of workload migration of all workload residing in Plano and Tulsa to achieve the consolidation. We will prioritize workload migrations, with Plano workloads into Tulsa taking the highest priority. This will allow the County to consolidate into Tulsa as quickly as possible to reduce the cost and complexity of operating in two data centers.

The HPES quality framework is wrapped around our Migration Factory. Using industry-recognized models, such as Software Engineering Institute's (SEI) Capability Maturity Model (CMM), International Organization for Standardization (ISO), Information Technology Infrastructure Library (ITIL), and Six Sigma, we continually focus on process and quality improvement. Our strong focus on quality and process excellence enables us to provide the high-quality, consistent migration services that the County requires.

Through quality assurance, we validate that data center migration processes are operating in "control." We monitor key process indicators, internal controls, and processes. Also, to verify the suitability and effectiveness of the quality management systems in satisfying customer quality objectives, our leadership reviews reports from internal, risk-based audits conducted throughout the year.

Note that pack-and-ship migrations may begin before the hybrid environment buildout is complete, if otherwise permitted by the County, since they do not require the hybrid environment to be in place in order to move. If we are able to ship servers before the Broker is in place, we will simply import those systems to the governance facility once the Broker is live to make them part of the hybrid environment at that time.

Migration activities follow step-by-step processes for the Dev/Test and production environments. During this phase, HPES will work with the County, our technical resources, and our application SMEs to execute the migrations from the source to the target environment. The migrations will be in accordance with the approved Migration Runbook Plan and approved detailed design documentation according to the

migration schedule for each move group. The contents will be captured in the Migration Runbook developed for each application. Tasks performed as part of the Go-To-Production process, such as executing hardening scripts, loading software agents for antivirus and adding the devices to the central repository, are incorporated into the project plan to make sure that the approved Go-To-Production process is followed for all migrations. Note that in the MPC environment, many of these tasks are automated, which will make the migration process more efficient.

During the migration, as assets migrate, their Resource Units will be recast from the current contract billing structure to the new contract billing structure. The County will not be billed for both in the same month.

We expect to employ multiple migration methods. Typical criteria to determine the proper migration method are the application downtime restrictions, amount of data to be migrated, network bandwidth, and any special security procedures that need to be followed. Our migration engineers, with the support of the County-designated project manager and application and infrastructure SMEs, will execute the Migration Runbook Plan according to the project schedule. The business owner of the application will provide the final approval during the cutover and is responsible for coordinating user acceptance testing and declaring the migration a success.

All migrations will have contingency plans to invoke a back-out or other service restoration procedure in the event of a failure, or a scenario where the migration is at risk of exceeding its allotted window. The TPM and the County business owner will mutually agree on the criteria for invoking the contingency plan.

The migration plan will include County freeze periods and adjust migration move groups accordingly, and will consider migration alignment with maintenance windows to minimize downtime. Migration of applications impacting critical services will be reviewed; we may invoke the contingency plan to mitigate impact on critical service supporting County business. Each move group plan will require County approval and participation by the application stakeholders in acceptance testing.

Automated tools like DoubleTake and PlateSpin will help mitigate or lower the downtime considerably, as migration can be performed while source servers are live: stakeholders can test on the target servers at a time convenient for them in most cases.

- Automated Tools – Automated systems and tools involved in proposed solution

We will provide the migration tool licenses, such as DoubleTake and PlateSpin. Some applications may be manually installed into the target data center for a number of reasons, including ease of configuration, the need to upgrade the version of the application, or the desire to have a clean install of the application in the target environment. The engineering and application teams will collaborate to make the decision for each application. Following the initial seeding, the County application team will test the application in the target data center. HPES recommends that the County participate in the performance of a full system and integration test to validate that the application is working as expected.

Our Migration Factory uses a tool from Binary Tree Company. HPES can provide large-scale migration support by planning and executing multiple move groups concurrently, consisting of multiple applications and associated components and using software products such as those described in Table 74.

Table 74. Automated Tools

TOOL NAME AND VENDOR	DESCRIPTION
DoubleTake	DoubleTake v7 is a migration tool that will be used for migration from Plano to Tulsa. DoubleTake performs a complete server copy from the source server onto the target server. It also has an advantage of having an asynchronous replication feature, significantly simplifying the data synchronization effort required during the final go-live process. Data synchronization can be set to certain files, directories, or file systems, optimizing the amount of data being transmitted on the network.
PlateSpin	PlateSpin v11 is a migration tool similar to DoubleTake and will be used for migrations into the County managed private cloud. PlateSpin performs a complete server copy from the source server to the target server, if needed. It allows source servers to be copied as an image that can be transported using an approved portable storage device and then restored to either a physical or virtual server on arrival at the Tulsa data center.

- Qualifications and Experience – Background and experience in comparable environments

HPES has more 40+ years of experience in data center transition and consolidation with a special emphasis on collaboration to add value. We will leverage our industry best practices, deep IT expertise, and our trusted, reliable, and repeatable services on behalf of the County. HPES delivers solutions that we know will work, are time-tested, and produce expected results.

Centers for Medicare and Medicaid Services (CMS) Enterprise Data Center (EDC) Contract: Using TTM, we executed a comprehensive transition in three parts.

- During the first year of our CMS EDC contract, we transitioned workloads from six different CMS data centers into our data center. Our transition team developed the plans and led the transition activities.
- We worked closely with all CMS business owners and the incumbent application hosting services provider to schedule migrations during times, and in a manner, acceptable to the legacy production data centers.
- We deployed start-up teams of experienced specialists, including design engineering, system administration, network engineering, security, backup and restore, and storage and monitoring experts.
- During the transitions, we implemented the move of a large number of workloads into our center. Concurrently, we supported overlapping workload transitions for Medicare Administrative Contractors (MACs), Durable Medical Equipment (DME) MACs, as well as workloads that previously completed the transition. To reduce risk, we used proven, repeatable processes and refined them from transition to transition.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

Storage Architecture (Schedule 2.1, Section 3.5)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary

The core of our primary Data Center Storage Architecture includes the latest innovation of HPE 3PAR enterprise storage, which is designed for both cloud and traditional environments. The storage hosts operating system images, virtual snapshots, and application data. Our architecture enables the server image to be disassociated from the physical hardware, allowing the image to move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover. Our managed Storage Architecture supports the applications that enable a more mobile workforce and citizen access to County services.

The Storage Architecture Transition project is a specialized and integrated component of the Data Center Consolidation, and our team will provide tight coordination with that project and its execution as well as with the implementation of the Colorado Springs Disaster Recovery (DR) implementation. Table 75 summarizes the types of storage in place in the County, the current and post-migration technologies in use for each, and the Transition strategy for each.

Table 75. Storage Transition Summary

TIER	CURRENT	FUTURE	TRANSITION APPROACH
1 (Data Center)	3PAR P10000 thick provisioned 15,000 RPM drives (Plano and Tulsa)	3PAR P20000 thick provisioned 10,000 RPM drives (Tulsa)	Replication, Peer Motion
1 (AT&T POP)	3PAR StoreServ 8400 2N Solid State drives	3PAR StoreServ 8400 2N Solid State drives	No change in Transition. We will review and re-address the architecture when this storage comes due for refresh.
2	3PAR P10000 thinly provisioned 15,000 RPM drives (Plano and Tulsa)	3PAR P20000 thinly provisioned 10,000 RPM drives (Tulsa)	Replication, Peer Motion
Archive	3PAR P10000 thinly provisioned 7,200 RPM drives (Tulsa)	3PAR P20000 thinly provisioned 7,200 RPM drives (Tulsa)	Replication, Peer Motion
DPC	3PAR 7200 with 10,000 RPM drives	3PAR 7200 with 10,000 RPM drives	No change in Transition. We will review and re-address the architecture when this storage comes due for refresh.
Immutable	EMC Centera SN4	EMC Centera Gen4LP	Replication
Email	Email is stored on the 3PAR in both Plano and Tulsa	Provided by the Microsoft Azure Government Cloud	E2E Complete™
Mainframe	HPE P9500 or equivalent in Plano (leveraged)	HPE P9500 or equivalent in Plano (leveraged)	None. Mainframe storage remains intact until the mainframe is decommissioned. At that time, the new midrange solution for those applications will have been

TIER	CURRENT	FUTURE	TRANSITION APPROACH
			deployed (under a separate project) using the appropriate tiers of SAN storage.
Direct-Attached	Disk drives installed on and dedicated to a physical server (types may vary)	Disk drives installed on and dedicated to a physical server (types may vary)	None specific to the storage environment. Direct attached storage will be replaced, and its data migrated to new storage at the time its associated server is refreshed.
Backups (Data Center)	HPE StoreOnce B6200 Virtual Tape Library (VTL)	HPE StoreOnce B6600 Virtual Tape Library (VTL)	Replication
Backups (DPC)	HPE StoreOnce D4212 at Rancho Bernardo MSL 4048 Tape Library	HPE StoreOnce D4212 at Rancho Bernardo Replicating to DR site in lieu of tape creation, for offsite storage	No Transition of VTL environment; only need to start replication to Colorado Springs Tape Libraries will remain intact until all tapes are expired.

For Storage Area Network (SAN) storage, we are currently providing a 3PAR P10000 in both Tulsa and Plano, with 15,000 RPM drives for tier 1 and 2 storage and 7,200 RPM drives for the archive tier. Tiers 1 and 2 of storage are redefined to reduce cost without sacrificing performance. The primary immutable storage (EMC Centera) is in Plano and is replicated to an EMC Centera in Tulsa. Document Processing Center 3PAR storage is available in the Viewridge and Lemon Grove San Diego sites. Our current backup solution provides a StoreOnce VTL in the data centers at Tulsa and Plano replicating to each other for offsite backup set protection and a combination of a smaller VTL in Rancho Bernardo with tape copies for offsite storage of backup sets. Our Transition solution addresses each of these types of storage.

The 3PAR 20000 is the latest innovation in enterprise storage from HPE. Primary data (all 3PAR-based tiers) for applications with a 48-hour Recovery Time Objective (RTO) is replicated to the DR site. The primary immutable storage will be located in the new production data center in Tulsa on refreshed EMC Centera storage and will be replicated to a refreshed Centera at the DR site. We are refreshing the 3PAR storage at the County's San Diego sites with like 3PAR storage to reduce the impact on operational processes and maintain the same level of performance. The backup solution also meets the requirements by providing a refreshed StoreOnce VTL in Tulsa and a smaller refreshed StoreOnce in Rancho Bernardo, both replicating to the DR site for remote storage of backup data. The backup solution changes from the current solution by replicating all data center backup data to the DR site and by eliminating remote offsite storage of backup data on tapes for the Rancho Bernardo site in favor off replicating that data to the DR site as well.

Rationale

To meet the increased capacity and transaction requirement of the consolidated data center environment and improve the storage architecture for primary SAN storage, we will transition to a refreshed, dedicated SAN with a 3PAR 20000 storage array. The 3PAR 20000 was selected to provide better performance than the current environment, with lower-cost disk drives. The current Tulsa and Plano storage environments typically reach a peak of approximately 2,450 KB per second, while the new design is capable of 2,438 MB per second—three orders of magnitude increase in performance headroom.

Our approach for all storage migrations taking place, both during and after Transition, is to provide improved storage performance and capacity at the point of refresh, without disruption to County business applications. Our Transition approach also makes sure that during the Transition period, data redundancy currently in place between Plano and Tulsa is re-established in the Colorado Springs DR site prior to removal of the Plano environment.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Depending on the type of storage and stage of the Transition, we will execute this project at the Tulsa and Plano data centers and our Rancho Bernardo site.

Our storage Transition engineers will come from HPES' US Public Sector delivery organization, a virtual team composed of U.S. citizens based in the Continental United States, working in close coordination with the local San Diego teams.

We will engage EMC Professional Services to install, configure, and migrate the existing immutable storage environment to the refreshed environment.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

Overall, we use a combination of host-based and storage-based replication to migrate data to the new storage and backup infrastructure without interruption to business processes and without data loss. Please refer to Section 2.9, Storage Services (response to Schedule 4.3, Section 6.12), Methodology and Key Processes, for additional information.

Transition Schedule and Tasks

As shown in Figure 165, HPES presents a notional transition schedule and Gantt chart, with high-level tasks, milestones based on a January 2, 2017 Contract Effective Date (CED). As previously noted, we will adjust the schedule based on the actual CED and final detailed plan. Task descriptions and key deliverables on the schedule are explained at a high level following the chart.

Plan, Procure, and Engineer (Design). HPES will create a detailed plan and design for the new storage architecture and provide engineering documents to migrate data from the original storage solution in Plano and Tulsa to the new storage solution in Tulsa and Colorado Springs (DR). We will submit the design and plan deliverables and review them with the County. The County will review and respond based on the agreed schedule. We will make any final revisions and create the detailed Bill of Materials from which we will procure the needed hardware, software, and services. All design deliverables will be posted to the Service Portal as required.

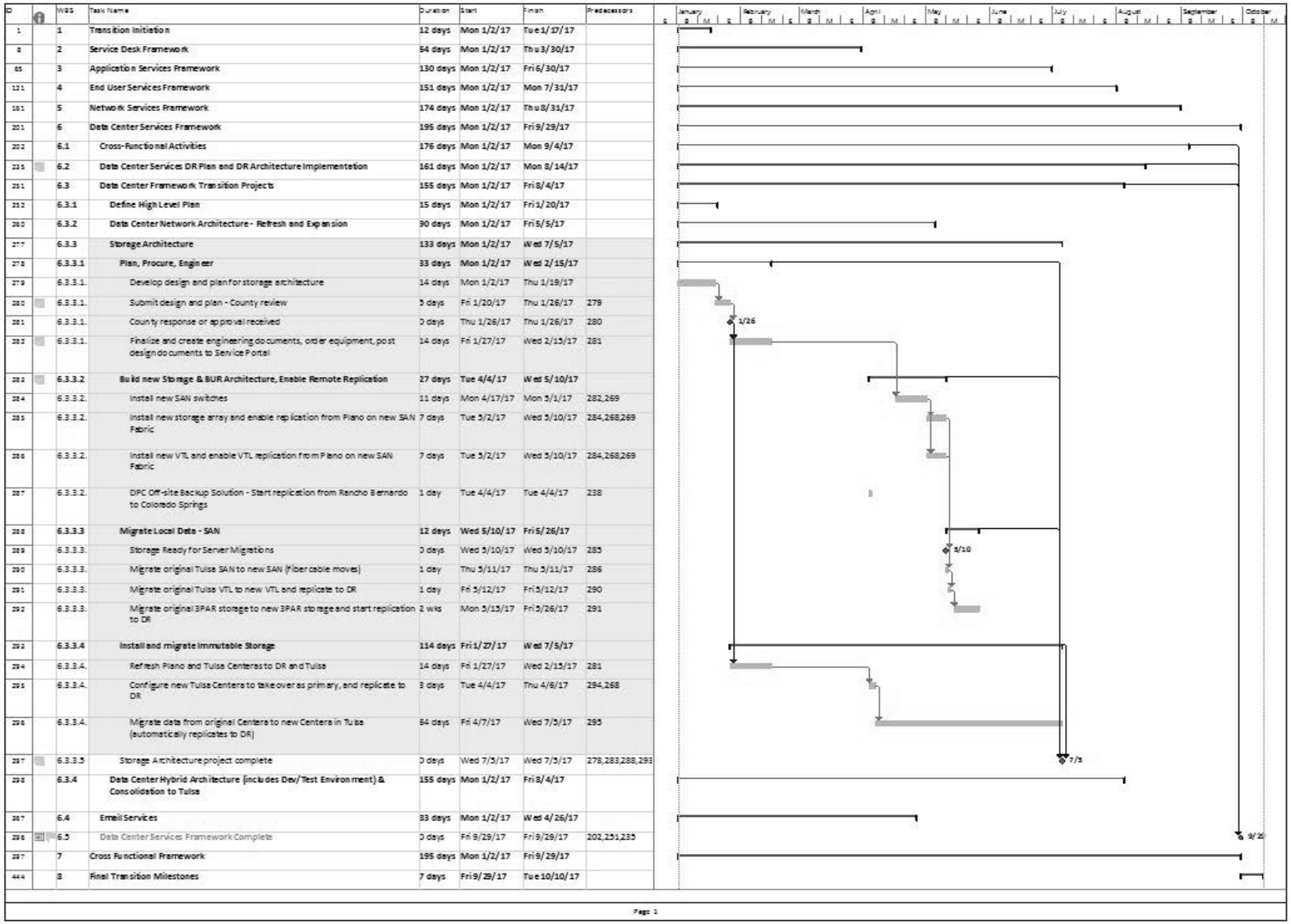
Build New Storage and Backup Architecture, Enable Remote Replication. Once hardware is received, we will begin the build process. We will install the new SAN switches, storage, and VTL in Tulsa, configure and test the environment, and begin the process of replicating data from the current Plano array and VTL to the new Tulsa array and VTL. Replication from Plano to Tulsa is continuous throughout the Data Center Consolidation project, and is turned down for each application at the point during the consolidation when all application data has been verified and accepted on its Tulsa system.

Preparation of the DR environment will also be occurring in parallel with the buildout at Tulsa. Once the DR environment is available, we will begin replication of SAN storage for applications that require DR with a 48-hour Recovery Time Objective (RTO), from the new Tulsa array to the DR site. We will replicate VTL data to the DR site for applications that require DR with a 72-hour RTO. We will begin replication of VTL data from Rancho Bernardo to the DR site for offsite storage.

We will engage EMC Professional Services to perform the Transition activities for Immutable Storage; this includes refreshing both Centera units. The new units will be located in Tulsa and in the Colorado Springs DR site. The new Tulsa Centera will be configured to take over as the primary, and will replicate to the Centera at the DR site. All existing Centera data will be replicated to the new Tulsa Centera. The Centera refresh/migration will not require downtime. However, to make sure there are no configuration problems after this refresh process, it is good practice and required by EMC that we reboot the Centeras shortly after refresh/migration. The reboot process will cause about one hour of downtime for the immutable storage service environment. We will coordinate this activity, like all Transition tasks, with the County via the Change Management process.

The rest of the Document Processing Center (DPC) storage and backup architecture will be refreshed at the appropriate time post-Transition—there are no tasks required during the Transition period.

Figure 165. Storage Transition Activities



ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	54 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
235	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
252	6.3.1	Define High Level Plan	15 days	Mon 1/2/17	Fri 1/20/17	
260	6.3.2	Data Center Network Architecture - Refresh and Expansion	90 days	Mon 1/2/17	Fri 5/5/17	
277	6.3.3	Storage Architecture	133 days	Mon 1/2/17	Wed 7/5/17	
278	6.3.3.1	Plan, Procure, Engineer	33 days	Mon 1/2/17	Wed 2/15/17	
279	6.3.3.1.	Develop design and plan for storage architecture	14 days	Mon 1/2/17	Thu 1/19/17	
280	6.3.3.1.	Submit design and plan - County review	5 days	Fri 1/20/17	Thu 1/26/17	279
281	6.3.3.1.	County response or approval received	0 days	Thu 1/26/17	Thu 1/26/17	280
282	6.3.3.1.	Finalize and create engineering documents, order equipment, post design documents to Service Portal	14 days	Fri 1/27/17	Wed 2/15/17	281
283	6.3.3.2	Build new Storage & BUR Architecture, Enable Remote Replication	27 days	Tue 4/4/17	Wed 5/10/17	
284	6.3.3.2.	Install new SAN switches	11 days	Mon 4/17/17	Mon 5/1/17	282,269
285	6.3.3.2.	Install new storage array and enable replication from Plano on new SAN Fabric	7 days	Tue 5/2/17	Wed 5/10/17	284,268,269
286	6.3.3.2.	Install new VTL and enable VTL replication from Plano on new SAN Fabric	7 days	Tue 5/2/17	Wed 5/10/17	284,268,269
287	6.3.3.2.	DPC Off-site Backup Solution - Start replication from Rancho Bernardo to Colorado Springs	1 day	Tue 4/4/17	Tue 4/4/17	238
288	6.3.3.3	Migrate Local Data - SAN	12 days	Wed 5/10/17	Fri 5/26/17	
289	6.3.3.3.	Storage Ready for Server Migrations	0 days	Wed 5/10/17	Wed 5/10/17	285
290	6.3.3.3.	Migrate original Tulsa SAN to new SAN (fiber cable moves)	1 day	Thu 5/11/17	Thu 5/11/17	286
291	6.3.3.3.	Migrate original Tulsa VTL to new VTL and replicate to DR	1 day	Fri 5/12/17	Fri 5/12/17	290
292	6.3.3.3.	Migrate original 3PAR storage to new 3PAR storage and start replication to DR	2 wks	Mon 5/15/17	Fri 5/26/17	291
293	6.3.3.4	Install and migrate Immutable Storage	114 days	Fri 1/27/17	Wed 7/5/17	
294	6.3.3.4.	Refresh Plano and Tulsa Centeras to DR and Tulsa	14 days	Fri 1/27/17	Wed 2/15/17	281
295	6.3.3.4.	Configure new Tulsa Centera to take over as primary, and replicate to DR	3 days	Tue 4/4/17	Thu 4/6/17	294,268
296	6.3.3.4.	Migrate data from original Centera to new Centera in Tulsa (automatically replicates to DR)	64 days	Fri 4/7/17	Wed 7/5/17	295
297	6.3.3.5	Storage Architecture project complete	0 days	Wed 7/5/17	Wed 7/5/17	278,283,288,293
298	6.3.4	Data Center Hybrid Architecture (includes Dev/Test Environment) & Consolidation to Tulsa	155 days	Mon 1/2/17	Fri 8/4/17	
367	6.4	Email Services	33 days	Mon 1/2/17	Wed 4/26/17	
396	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
397	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

Migrate Local Data – SAN. Once the new SAN and Backup environment are fully configured and ready to support live servers, the various migrations described in the Consolidated and Single Data Center section can begin. In addition to supporting these migrations, servers that are not migrating (that sit in Tulsa currently) must also have their storage migrated to the new environment. Note that there are no dependencies between the Data Center Consolidation and migration of the current Tulsa servers to the new storage—these two activities can occur in tandem.

To migrate the Tulsa environment from the current to the new storage, we will first verify that all data is fully synchronized from the existing array. The SAN has redundant connectivity, and we will take advantage of this redundancy to move the environment from the current to the new SAN without requiring an outage to the systems or applications. We will move one set of connections from the current fabric to the new fabric, switch data access to the new fabric, then move the second set of connections to the new fabric. We will then enable replication of these volumes to the DR site.

In the current storage architecture, end-user data storage is available primarily through network attached storage (NAS) shares that are mapped to workstations as the end users' H: drives for their personal shares and S: drives for their group shares. In the current architecture, NAS appliances using 3PAR storage arrays for end-user data storage are located in Tulsa and are also available in Plano. In some special circumstances, end-user data storage is also available through server shares using 3PAR storage to access AutoCAD drawings and mapping data for example.

As previously noted, HPES and the County will strive to migrate End-User data to OneDrive for Business in order to avoid having to migrate it to the new array as well. If the End-Users cannot commit to the four-month timeframe required, and the County does not wish to elongate the timeframe for the Data Center Framework Transition, we will build out the End-User NAS shares by providing End-User data storage directly from the new NAS-capable 3PAR, eliminating the need for NAS appliances. This change will be transparent to the users.

Following successful completion of the Storage Architecture Transition, HPES will securely destroy all data on the retired storage and backup systems and provide disposal of those items.

- Automated Tools – Automated systems and tools involved in proposed solution

Both the backup storage (VTL) and 3PAR have native replication capabilities built into and enabled by the storage array software. When host/system-based replication is used, DoubleTake V7 will be the tool that migrates the data along with the server image. This is described in the Consolidated and Single Data Center section. Table 76 lists storage-based tools and utilities.

Table 76. Storage-Based Tools and Utilities

TOOL	DESCRIPTION AND USAGE
VTL Utilities	StoreOnce replication using Catalyst Replication of deduplicated backup data reduces time and bandwidth on the dedicated replication link between Tulsa and the DR site. Backup data is available for DR more quickly, to reduce the chance of missing backup data in case of a DR event.
3PAR System Utilities	• 3PAR array-based replication allows background replication of storage from one array to another and will aid the migration of service data from Plano to Tulsa. • 3PAR Storage Peer Motion allows us to migrate storage data volumes off the old Tulsa 3PAR onto the new Tulsa 3PAR without any interruption in accessing the data.

- Qualifications and Experience – Background and experience in comparable environments

Table 77. Relevant Experience

QUALIFICATIONS AND EXPERIENCE CITATION	WHAT WE DO AND HOW IT IS RELEVANT TO THE COUNTY
County of San Diego	Upgraded storage architecture in 2012 using a similar process and methodology.
NGEN	• On the Department of Navy (DON) Next Generation Network (NGEN) contract, which includes support for the Navy Marine Corps Intranet (NMCI): • From 2005 until early-2014, our team managed and monitored a diverse SAN environment that consisted of two different vendors. • In mid-2014, the team designed, engineered, and implemented a one-platform SAN storage environment to standardize NMCI on the more flexible, easier to use and support NetApp SAN. This single-SAN approach enabled us to capitalize on native capabilities to provide site-to-site resiliency and reduce backup overhead through a storage hub and tapeless backup. Our single-SAN design is reducing complexity and Total Operating Cost (TOC) while increasing operating efficiencies and effectiveness.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

Service Portal (Schedule 2.1, Section 3.6)

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary

HPES' End User Access (EUA) solution, integrated closely with our Service Management systems (Service Manager), will provide a centralized Service Portal for all County users. Our Service Portal provides access to self-service assistance options and multiple dashboards easily accessible by County users, Service Desk agents and HPES support teams. It is mobile-enabled and easy to use. Additional information regarding the Service Portal design and functionality is found in Section 2.6

During the Service Desk Transition, which occurs during the first 90 days from CED, we will set up the core Service Portal functionality, including single sign-on, and link it to current data sources and source systems to integrate with the current repositories.

Rationale

Our Portal implementation approach is one that has been used at other accounts with a high degree of success. We have a repeatable process for the base Portal setup, which is being proposed here. We limited the initial deployment to the base set of configuration elements to minimize risk and to give both the County leadership and HPES a chance to solicit user feedback and suggestions to feed a continual improvement plan for the Portal's ongoing evolution.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES will work with the County Technology Office (CTO) and its designees to assist in the design and testing and governance of the Service Portal. Our Global Engineering and Technical Consulting (GETC) organization, which has experience implementing similar projects for other customers' portal requirements, will provide the engineering and customization work, in collaboration with the County's local engineering and support team, which manages the current portals. We will hold design sessions with the County at HPES's Rancho Bernardo facility or at a designated County location.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

HPES will use infrastructure project management processes in delivery of the project, as described in Section 2.5.7 of this proposal.

Transition Schedule and Tasks

Figure 166, on the following page, provides a notional view of the activities associated with the Service Portal Transition.

Design Customizations. The Portal configuration process is an Agile-style iterative process providing rapid feedback throughout. At the start of the project, we will collaborate with the County in several iterative workshops to design the Portal "look and feel" and to review initial functionality. The configuration process that takes place during the Transition period will include items such as the following:

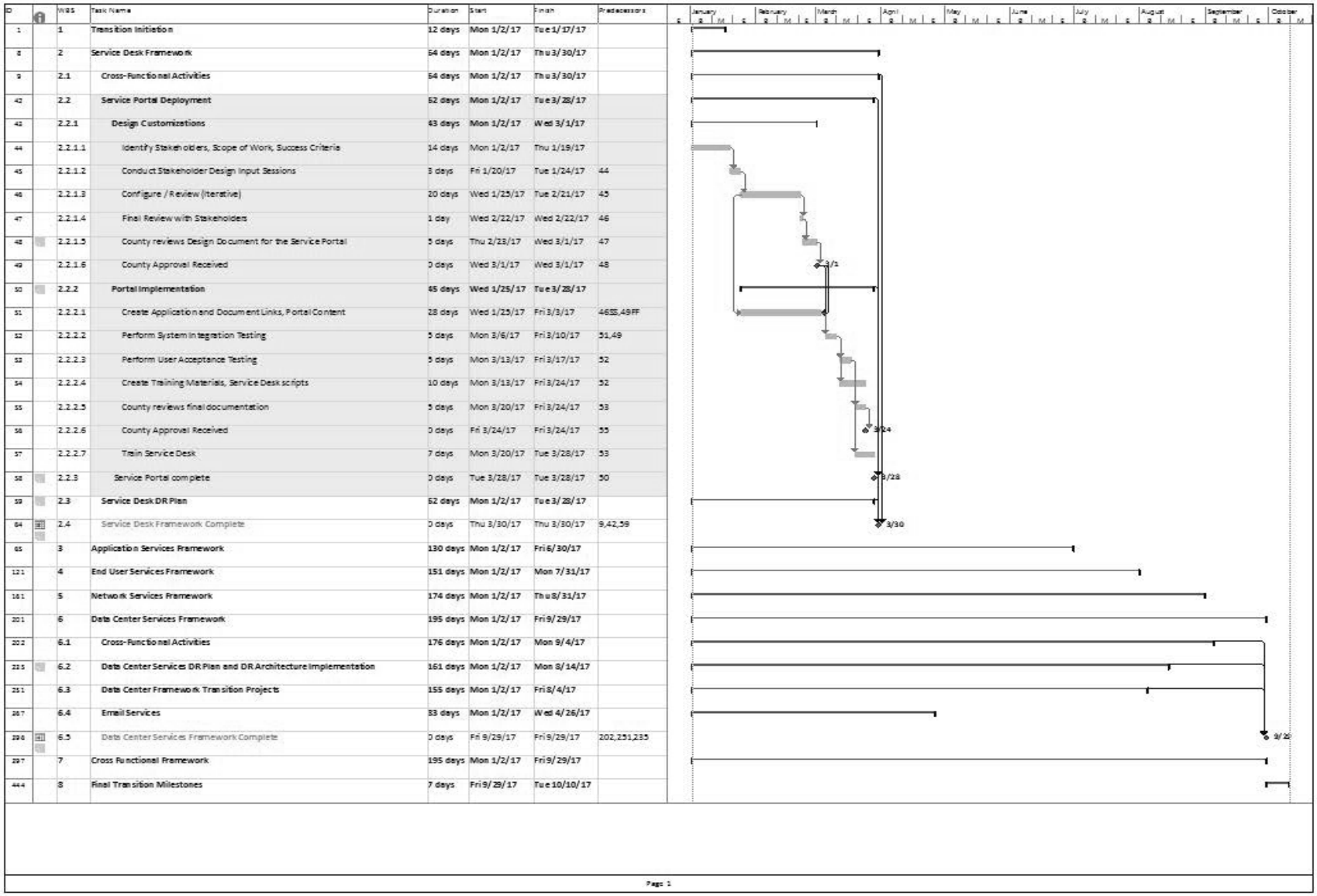
- County branding and "look-and-feel" elements on the front page (tiles, menus, links)
- Use of banners and splash pages
- Identification of user roles to be configured, to determine which groups have access to the various types of information
- Integration with Active Directory for Single Sign-on and configuration of user roles
- Integration with Service Manager and other tools
- How existing portals and data sources (ITSC, Doc Vault, and so forth) will be presented—as links or tiles from the main page to the existing functioning applications.

Service Portal Implementation. During transition, Portal implementation has two parts: (1) the "look and feel" of the Portal and (2) integrating HPE Service Manager (SM) and other applications and data sources. We begin with a sample portal, such as the one shown in Section 2.6, and gather feedback from the County to determine their preferences. This is an iterative process, and once finalized and approved by the County it becomes the Transition release design version.

With Portal design in hand, the next task is to connect the functionality of the document repositories and portal systems in use today to the appropriate tiles or links in the new Portal design. The integration of Service Manager with the Service Portal is part of HPES's product integration; that is already complete. The functionality in the Portal that is embedded in Service Manager will require minimal configuration. For Transition, there will be no change in the application functionality of existing source applications that

sit behind the Portal (those reached by pass-through links and that are not part of the Service Manager suite).

Figure 166. Draft Service Portal Transition Activities



ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17	
9	2.1	Cross-Functional Activities	64 days	Mon 1/2/17	Thu 3/30/17	
42	2.2	Service Portal Deployment	52 days	Mon 1/2/17	Tue 3/28/17	
43	2.2.1	Design Customizations	43 days	Mon 1/2/17	Wed 3/1/17	
44	2.2.1.1	Identify Stakeholders, Scope of Work, Success Criteria	14 days	Mon 1/2/17	Thu 1/19/17	
45	2.2.1.2	Conduct Stakeholder Design Input Sessions	3 days	Fri 1/20/17	Tue 1/24/17	44
46	2.2.1.3	Configure / Review (Iterative)	20 days	Wed 1/25/17	Tue 2/21/17	45
47	2.2.1.4	Final Review with Stakeholders	1 day	Wed 2/22/17	Wed 2/22/17	46
48	2.2.1.5	County reviews Design Document for the Service Portal	5 days	Thu 2/23/17	Wed 3/1/17	47
49	2.2.1.6	County Approval Received	0 days	Wed 3/1/17	Wed 3/1/17	48
50	2.2.2	Portal Implementation	45 days	Wed 1/25/17	Tue 3/28/17	
51	2.2.2.1	Create Application and Document Links, Portal Content	28 days	Wed 1/25/17	Fri 3/3/17	46SS,49FF
52	2.2.2.2	Perform System Integration Testing	5 days	Mon 3/6/17	Fri 3/10/17	51,49
53	2.2.2.3	Perform User Acceptance Testing	5 days	Mon 3/13/17	Fri 3/17/17	52
54	2.2.2.4	Create Training Materials, Service Desk scripts	10 days	Mon 3/13/17	Fri 3/24/17	52
55	2.2.2.5	County reviews final documentation	5 days	Mon 3/20/17	Fri 3/24/17	53
56	2.2.2.6	County Approval Received	0 days	Fri 3/24/17	Fri 3/24/17	55
57	2.2.2.7	Train Service Desk	7 days	Mon 3/20/17	Tue 3/28/17	53
58	2.2.3	Service Portal complete	0 days	Tue 3/28/17	Tue 3/28/17	50
59	2.3	Service Desk DR Plan	52 days	Mon 1/2/17	Tue 3/28/17	
64	2.4	Service Desk Framework Complete	0 days	Thu 3/30/17	Thu 3/30/17	9,42,59
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
161	5	Network Services Framework	174 days	Mon 1/2/17	Thu 8/31/17	
201	6	Data Center Services Framework	195 days	Mon 1/2/17	Fri 9/29/17	
202	6.1	Cross-Functional Activities	176 days	Mon 1/2/17	Mon 9/4/17	
215	6.2	Data Center Services DR Plan and DR Architecture Implementation	161 days	Mon 1/2/17	Mon 8/14/17	
251	6.3	Data Center Framework Transition Projects	155 days	Mon 1/2/17	Fri 8/4/17	
267	6.4	Email Services	83 days	Mon 1/2/17	Wed 4/26/17	
296	6.5	Data Center Services Framework Complete	0 days	Fri 9/29/17	Fri 9/29/17	202,251,235
297	7	Cross Functional Framework	195 days	Mon 1/2/17	Fri 9/29/17	
444	8	Final Transition Milestones	7 days	Fri 9/29/17	Tue 10/10/17	

Testing. With the design complete and built, the Portal and attached functionality can be tested. We use the testing methods used for other infrastructure and applications releases, progressing from Systems Integration Test (SIT) through User Acceptance Test (UAT). These test steps are described in more detail in Sections 2.7 and 2.10.

Content Development, Content Migration, and Training. In the same timeframe as the testing phases, we will create Service Desk related content, such as self-help content (videos, tip sheets, and so forth) and cross-functional content associated with the Service Desk (refer to Section 2.11, Cross Functional Framework Transition, in response to Schedule 2.1, Section 3.1), available on the Portal. We will create Service Desk scripts and conduct training for the Service Desk agents to support the Service Portal, and work with the County to develop training and communications materials to introduce users to the new capabilities.

At the end of the process, we will present final documentation and the Portal itself for County review and response. Approval and successful completion of the activities above will mark the end of the 90-day Service Desk Framework Transition. During the rest of the framework transitions, reports, updated process documentation, design documents, and other deliverables will be posted to the Service Portal as these deliverables are completed.

- Automated Tools – Automated systems and tools involved in proposed solution

The Service Portal is customized using EUA and other web development tools.

HPES will use Project and Portfolio Management Center (PPMC) as our Primary Project and Portfolio Management (PPM) tool suite. We use PPMC for the development and ongoing management of project schedules.

- Qualifications and Experience – Background and experience in comparable environments

HPES has deployed thousands of client portals across the globe. We will apply our expertise in portals and collaboration, application transformation, and technology innovation to support the County's mission of providing a centralized and continuously managed focal point for all communications and information. Some examples include the following:

County of San Diego: HPES performed a successful transition from Northrop Grumman in 2011, including support for the existing myRequests portal. We subsequently established the ITSC portal, MASL Dashboard, and several SharePoint-based portals for both the County's and our own internal use.

Worldwide Power and Gas Company: HPES helped this company improve efficiency and customer satisfaction by integrating multiple supplier catalogs into a single integrated portal, with a friendly consumer-like experience for their employees. The number of service desk activities declined by about 15%, thanks to workflow enhancements that eliminated some manual activities and the generalization of dynamic forms so users no longer need to call for additional information.

Federal Healthcare Agency: HPES developed and integrated a medical portal for a client supporting a major hospital facility with full Health Information Privacy and Accountability Act (HIPAA) compliance.

Procter and Gamble: HPES implemented the EUA Portal for P&G users.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

High Level Transition Milestones and Tasks (Schedule 2.1, Section 4)

Estimated timeframes for each task are shown in Table 78 through Table 84. Timeframes are shown as "CED + x" where "x" is a number of calendar days from the Contract Effective Date. As previously noted, actual timelines will be adjusted based on detailed planning and mutual agreement with the County. Tasks that do not have to be performed by HPES are shown as "N/A".

Table 78. Transition Start-up and Organization

TASK	DUE DATE	TRANSITION MILESTONE
1. Each party shall assemble and name a transition management team for each Service Framework, including overall transition managers responsible for oversight of the entire transition process for each party.	CED	
2. Deliver to the County a detailed process and communications strategy for soliciting, making offers to, and hiring personnel used to perform the services.	N/A	
3. Propose, finalize and implement the communications and governance plan for the County and the County's Legacy Provider.	CED+10	
4. Conduct kick-off meetings with the Legacy Provider's disentanglement teams and the County's transition teams.	CED+17	

Table 79. Service Desk Framework

TASK	DUE DATE	TRANSITION MILESTONE
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	CED +30	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services	N/A	

TASK	DUE DATE	TRANSITION MILESTONE
(including any applicable Cross-Functional Services) to the County under this Service Framework.		
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	CED+20	
9. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+30	
10. Submit for County approval the design document for the Service Portal	CED+50	
11. Finalize and deliver the Service Portal. Add Service Desk related content to the Service Portal	CED+85	
12. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	Effective Date+ 90 days	Yes

Table 80. Application Services Framework

TASK	DUE DATE	TRANSITION MILESTONE
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-	N/A	

TASK	DUE DATE	TRANSITION MILESTONE
Functional Services to the County under this Service Framework, as applicable) and make offers to same.		
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	CED+45	
9. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+60	
10. Add Applications Services related content to the Service Portal	CED+90	
11. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	Effective Date+ 180 days.	Yes

Table 81. End-User Services Framework

TASK	DUE DATE	TRANSITION MILESTONE
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	

TASK	DUE DATE	TRANSITION MILESTONE
4. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
5. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
6. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
9. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	CED+60	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+75	
11. Add End-User Services related content to the Service Portal	CED+90	
12. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	Effective Date+ 210 days.	Yes

Table 82. Network Services Framework

TASK	DUE DATE	TRANSITION MILESTONE
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date	

TASK	DUE DATE	TRANSITION MILESTONE
	minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	CED+60	
9. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+75	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+75	
11. Add Network Services related content to the Service Portal	CED+90	
12. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	Effective Date+ 240 days.	Yes

Table 83. Data Center Service Framework

TASK	DUE DATE	TRANSITION MILESTONE
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
9. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	CED+200	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+230	
11. Add Data Center Services related content to the Service Portal	CED+240	
12. Submit for County approval the design document for the E-Mail Service	CED+30	
13. Submit for County approval the design document for the Development and Test Environment	CED+45	

TASK	DUE DATE	TRANSITION MILESTONE
14. Submit for County approval the design document for the Consolidated Data Center	CED+45	
15. Submit for County approval the design document for the Storage Architecture	CED+20	
16. Develop and Deliver E-Mail Services	CED+120	
17. Develop and Deliver Development and Test Environment	CED+180	
18. Develop and deliver Consolidated Data Center	CED+210	
19. Develop and deliver Storage Architecture	CED+180	
20. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	Effective Date+ 270 days.	Yes

Table 84. Cross Functional Service Framework

TASK	DUE DATE	TRANSITION MILESTONE
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	

TASK	DUE DATE	TRANSITION MILESTONE
7. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
9. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	CED+180	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross- Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	CED+210	
11. Develop and deliver to the County for approval a completed Management Plan for each Cross Functional Component	CED+210	
12. Add all Cross Functional Services content to the Service Portal	CED+240	
13. Add all Cross Functional Management Plans to the Service Portal	CED+240	
14. Implement and deliver each Cross Functional Management Plan	CED+240	
15. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	Effective Date+ 270 days.	Yes

Executive Summary

Including Cross-framework/component integration, Competitive Differentiators and County Benefits

As your partner in delivery of IT Services for more than 10 years, HPES offers the County the lowest risk transition:

- We will not have to perform knowledge transfer, asset transfer, people transfer or spend time on these activities: our Transition period is fully dedicated to the success of your projects.
- Normal operations and your current projects will continue during the Transition period with no disruption or handoff required.
- Sixty percent of the Data Center Framework is already located in our target site for the Data Center Consolidation and will not have to move.
- There is a high degree of interdependency between the various Data Center projects. Only HPES has the depth of knowledge to fully comprehend these complexities from the start, and make sure that they are all accounted for, so that all of your projects execute flawlessly, on time and within budget.

Starting with Cathy Varner and throughout the organization, we are committed to sustaining excellence in support of, and in cooperation with the County. We will use our TTM and dedicated Transition Management team to complete the details behind the high-level Transition Plan used for illustration in

this section, and to provide the County with the governance, communications and documentation required to keep all stakeholders informed and confident of success. Both our local team and our teams of technical subject matter experts are ready to transition and deliver the County's next generation of IT services.

"Transition [from NG to HP as a prime] was a non-event. It was managed very well by HPES. There was zero impact to the County. There wasn't a whole lot to do from a project management perspective on the County side. HPES took on all the heavy lifting and they made everything transparent. It was a magnificently successful transition for the County."

County of San Diego Executive

The HPES plan meets all of the transition requirements as demonstrated in our response to Schedule 2.1, Section 2. We look forward to continuing our relationship with the County and are excited about the transition to the new Contract.

2.12 Transformation Services

Executive Overview

The County has achieved great success with numerous transformational activities, from DEH's Hazardous Material Division (HMD) receiving an outstanding innovation award for their e-Forms solution, to modernizing the annual enrolment process for employees, and the PUMA Mobile Probation Officer app which has received national recognition and awards. HPES is privileged to be your partner in these achievements and looks forward to partnering with you to transform the County to the next level of technology and services.

Continual improvement in the delivery of County services to its customers, which include residents, businesses, and visitors, requires the right balance among financial, social, environmental, and technology implementation objectives and a culture that is progressive and adaptive. We recognize that transformation is broader than technology identification and integration – it requires foresight, planning, and alignment with the business strategy to help the County continue to move forward.

We follow a bi-modal approach to proactively assess, deliver and sustain transformational IT initiatives, with one mode focused on stability and the other on agility. Mode 1 is planning and adhering to disciplined processes to ensure that business technology functions appropriately and securely. Mode 2 focuses on innovation, looking at new IT trends and early adoption of innovation that can be evolved and rolled-out quickly to manage cost and improve County effectiveness.

HPES will control transformational projects through Enterprise Architecture (EA) governance processes that incorporate CTO Architecture Principles, Bricks, reference patterns, technology assessments, regular meetings and roadmaps to identify and align solutions suitable with County business and IT strategic direction. HPES' CTA and our EA team will continue to champion innovation days and technology seminars, focusing on improvements to keep the County moving forward. Establishing actionable roadmaps with measurable objectives enables us to forecast and accommodate business changes in an agile orientation through effective governance and processes that:

- Use EA tools such as MEGA to create artifacts to identify, allocate, and measure transformational initiatives from an end-to-end perspective
- Establish a Transformational Maturity Model (TxMM) and analytical algorithms to analyze, predict, and recommend architectural and transformational initiatives
- Establish a Model Driven Enterprise in which service models are used to simulate and test emerging value chains and alternatives and accomplish prototyping and testing without impacting operational baselines
- Incorporate recommendations based on bi-modal organizational thinking.
- Blend bi-modal approaches to build County services from an "Outside-In" perspective.

Our approach to long-term transformation goes beyond those projects identified in Exhibit KK. We will leverage our knowledge of the County environment, business processes, and strategic objectives, with the foresight necessary to adapt to changes in the environment and foster citizen engagement. We propose two additional transformational projects for consideration: 1) Enterprise Information Management (EIM) to enable the County to take full advantage of the information it has to improve decision-making and make richer programs available to the public; and 2) Comprehensive Applications Threat Analysis (CATA) services to build security into applications from the start to minimize risk.

Transformational changes present challenges and opportunities to improve business execution, service quality, and innovations, with the right mix of current, emerging, and disruptive initiatives. We respect the past, understand the current environment, and have the vision to identify additional transformation initiatives taking advantage of flexible interfaces and extensible platforms to bridge transformational

gaps, eliminating barriers to change. HPES will partner with the County to continually transform, proactively and collaboratively, to improve the experience of County employees, taxpayers, and residents.

2.12.1 Transformation Services (Exhibit KK, Section 2.4, 2.5, 2.6)

- Key Considerations and Potential Alternative Approaches

HPES has worked diligently with CTO staff under the current contract to introduce positive changes in the environment through both new business processes and new technology. Some examples include:

- Technology Innovation Workshops, hosted by HPES to collaborate with and inform the County on key technologies. These include an Identity Workshop, which resulted in establishing the PKI vision, and Active Directory Workshop that resulted in Active Directory, Active Directory Federation Services and SCCM upgrades, as well as the DNS Re-Architecture using Akamai.
- Developed HP Cloud Strategy Roadmap detailing the vision to move from the current Tulsa/Plano state, to the mid-term state with HP Helion Cloud, and Goal state in a hybrid/broker environment. This initiative resulted in implementation and adoption by county for PaaS infrastructure hosted in the Rancho Bernardo Lab and HP Helion Cloud, and serves as the foundation to further support the County's move to hybrid and broker environments.
- Upgraded network perimeter security to provide secure, redundant firewall, SSL offloading, and load-balancing, which enabled the County to simplify and better secure its network landscape by retiring redundant and aging infrastructure in Microsoft ISA and Universal Access Gateways (UAGs).
- HPES provides the County a full range of mobile delivery capabilities to empower County field workers with native Android/iOS developed apps, to engaging citizens through mobile-friendly responsive web sites (Beach & Water, County Web Portal, Live Well Portal) to create a positive customer experience.
- Standardized the County architecture methodology using HPE's RightStep/TOGAF to provide a consistent framework to organize and define solution architectures, which has improved the overall quality and consistency of project deliverable. Institutionalization of standardized architecture Solution Design Documents (SDD) has improved speed to delivery by enabling quicker County approval, project start, and solution execution by downstream delivery teams.
- *Standardized solution assessment approach to quickly provide architecture direction* taking into consideration five categories: Cost, Business Fit, Architecture Fit, Quality, and Risk, to recommend the best solution to the County. This approach directly aligns with the County's focus on fiscal stability, operational excellence, and commitment to service improvement.

We will build upon these achievements to identify additional transformational initiatives and work collaboratively with County leadership and stakeholders to determine the feasibility of these initiatives. We do not anticipate potential impacts to the agreement to move forward with these types of initiatives.

In the following section, we describe our approach for driving Transformation as a program; then address specific transformational initiatives.

- Solution Summary and Rationale

Our transformational program will be based on the following tenets:

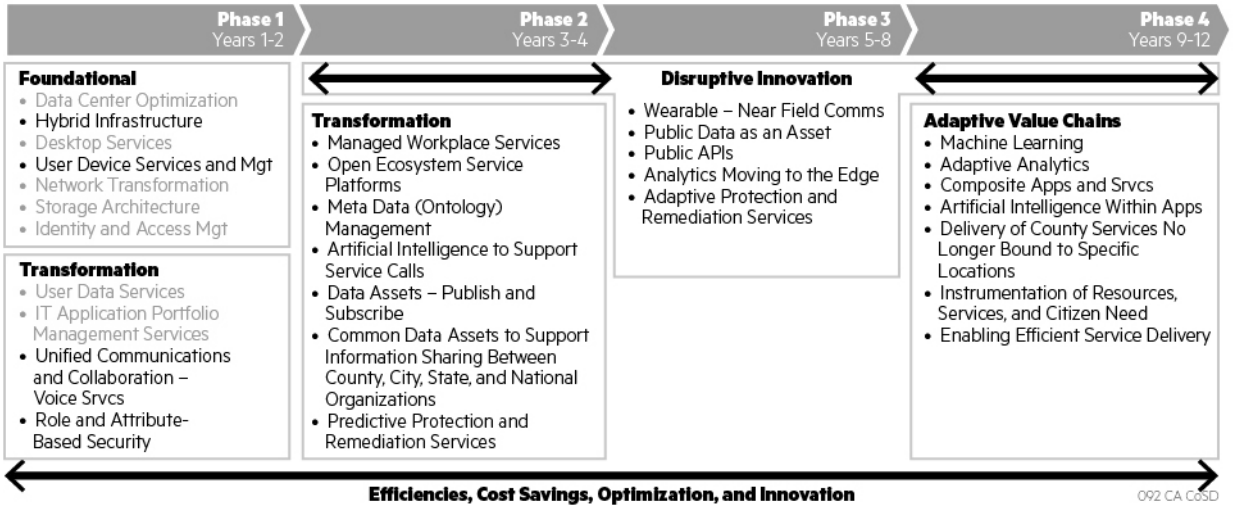
- **Enable citizen engagement (digital first) –** The County has recognized a growing preference among citizens to interact with the government online, at a time and place that is convenient for them, and they expect their experience to mirror that of the private sector. Tools, functions, capabilities, and services produced by transformational activities will allow the County to expand the current "digital first" initiative.

HPE's hybrid foundational platforms and services will enable the County to deliver additional services that align with citizen expectations. Embedding knowledge-based tools into existing systems and websites

enables citizens and employees to conduct transactions quickly and accurately. Whether in one-on-one scenarios or via social communities, County departments can learn from each interaction and tailor content to maximize effectiveness. This will improve citizen satisfaction, while minimizing the inconvenience of making a phone call or visiting an office.

- **Provide Secured Information Sharing and Enrichment (Open Data Platforms) –** Open Data Platforms (published APIs and consumable data marts) provide a secured and authoritative means to share and enrich information among County departments to proactively deliver services. Seamless interoperability drives mobility capabilities and a digital environment, increases the ability to share, reuse and analyze data, leading to creation of information and knowledge. An example of a use case enabled by these core capabilities would be to provide the County with means to dynamically identify, track, and interact with homeless veterans in the field. Or, instead of simply reacting to a distressed parent calling to report health symptoms, a predictive model could alert health officials based on the means to collect, correlate, and analyze data from health providers, pharmacies, and geospatial indications to notify citizens proactively with information and access to services. Treating data as an asset requires actively taking initiatives to improve both the quality and the usefulness of the data.
- **Adaptive Enterprise –**HPES offers a comprehensive Adaptive Enterprise strategy that we designed to strengthen every link in the County's value chain. Together, the components of our multifaceted Transformational Agenda fully address the County's business objectives. The County can achieve enterprise agility and growth while improving its overall return on IT investment (RoIT).

Figure 167. Transformational Agenda for the County



HPES' transformational agenda supports achieving the Future of the County

We will make sure that each transformational activity produces qualitative and quantifiable returns to the County. The following are complementary Transformational Categories:

- **Managed Workplace Services**– Provides services, platforms, and support that enable workers and citizens to interact in an effective way to create, manipulate, and access desired services from an authorized device or location – accommodating new value chains. [Tools and Devices]
  - User Device Services and Management
  - Desktop Services (Windows10, other mobile OSs)
  - User's operational device/environment is contextually aware
  - Unified Communication and Collaboration
  - Internet of Things (Wearable – Near Field Comms)

  - Artificial Intelligence to support Service Calls

- **Enterprise Information and Knowledge Management (EIKM) –** New capabilities and services oriented around the use of proactive analytics and public data as an asset. [APIs, consumable data assets]
  - Public Data as an Asset
  - Metadata (ontology) Management
  - User Data Services
  - IT Application Portfolio Management Services
  - Publish and subscribe data assets that support information sharing (contextual and semantic apps and services)
  - Analytics moving to the edge
  - Machine learning

We address the following considerations to effectively deliver the business value derived from transformational activities:

- **Strong focus on architecture foundation:** Rigor across the architecture-analysis-design-construction phase. This methodology advocates the establishment and evolution of reference architecture and applies a solution architecture for improved system-wide integration.
- **Importance of metadata:** A specialized metadata work stream manages metadata as a critical County asset. The common aspect associated with the digital workplace and the County's transformational initiatives is the maturity of data – information – knowledge – intelligence that directly enhances the County worker's ability to create and deliver services.
- **Not limited to a predetermined technical platform:** Use best-fit technologies to implement transformational solutions, including a technology-neutral approach independent of vendor solutions. Tool-specific best practices are introduced through technology extensions.
- **Modular and flexible to meet various size and complexity needs**: This approach adapts to projects of various sizes and complexities, customized to meet specific needs. Related subsets of activities are independently executed along phases or activity work streams, depending on project scope.

- Resources and Facility Approach Summary

HPES team members in Rancho Bernardo, including our CTA, and AT&T staff at Trade Street are dedicated to supporting the County, will have the lead to identify potential transformational projects because of their first-hand knowledge of the environment, culture, and strategic objectives. This team has reachback to corporate HPES and corporate AT&T resources with extensive expertise across services. This is not to say that *only* HPES CTA and AT&T can identify transformational projects—any and all members of the HPES and AT&T team can do so.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

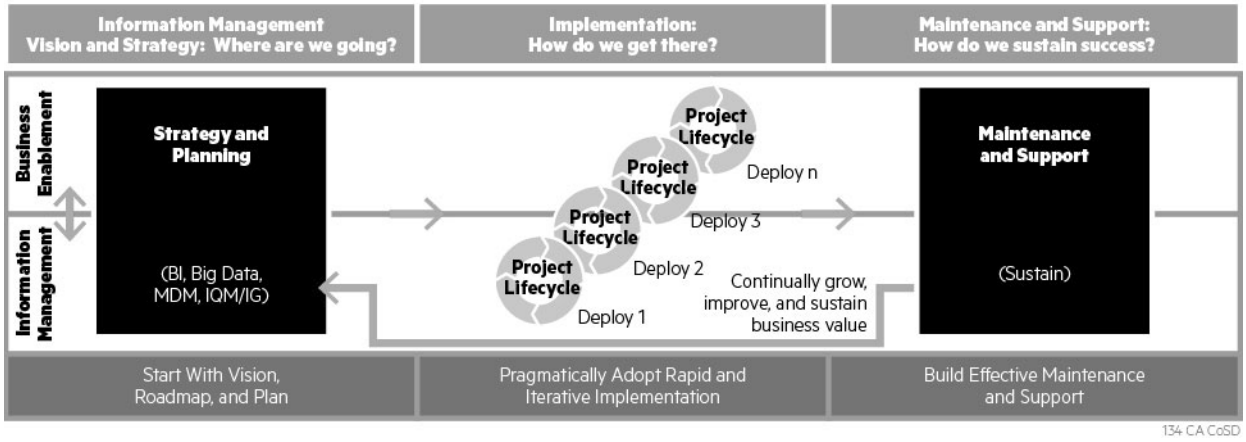
We are committed to making certain that transformation continues in the future, after successful completion of the identified transition and transformation projects. We will provide leadership and oversight for transformational projects through an Enterprise Architecture (EA) governance process that focuses on regular technology assessment, new ways to do business through online services and automation, and briefings for the County on new and evolving technologies and business processes. As part of our support of EA through our architecture team, we will present innovation days and technology seminars to keep a focus on improvements and new technologies to keep the County moving forward.

The HPES IT Solution Architecture (ITSA) applies industry-recognized reference architectures and patterns, described in Section 2.5.6 of this proposal, to the management of the transformational life cycle to provide successful and sustainable delivery and the highest value for the County. Consistent and

repeatable processes set clear expectations, simplify implementation, accelerate development, minimize errors, lower costs, reduce risk, and encourage strategic alignment between IT and the business.

The HPE Transformational Implementation Methodology (TIM) is an Agile methodology that facilitates discovery and prototyping for early insight into proposed transformational initiatives and solutions Figure 168. We use this tool-driven approach to rapidly perform transformational implementation activities in a highly productive, coherent, repeatable, and accountable manner.

Figure 168. HPES Transformational Implementation Methodology



This structured approach helps to continually grow and sustain business value.

The project lifecycle circles highlight the incremental release aspect of the business transformational life cycle. Each circle represents an incremental build and deployment, and the progression from the circle on the bottom (Deploy 1) to the circle at the top (Deploy n) represents the increasing complexity and scope involved, building on what was completed before, and the passage of time.

This methodology is composed of a rich array of features that support successful business intelligence (BI) implementation:

- **Iterative development support:** TIM leverages iterations on program, project, and activity levels, controlling progress via activity entrance and exit criteria.
- **Agile development from conceptual through logical and physical design:** TIM creates a conceptual and logical solution through the business requirements, architecture, and analysis phases. Agile development continues with a high-level physical design through the design, construction, testing, and deployment phases.
- **Reinforcement for business value:** The methodology uses project charter, interactive requirements gathering, and prototyping. Business objectives and ongoing business involvement are clarified throughout the systems development life cycle for transformational activities and systems.
- **Well-structured and content-rich:** The implementation framework includes methodology phases, activities, tasks; artifact/working document templates and samples; and clearly defined roles and responsibilities with supporting Responsible, Accountable, Support, Consulted, and Informed (RASCI) assignments.
- **Built-in support for critical information quality and information governance:** TIM embeds information quality and governance into implementation activities and tasks, and addresses organizational elements supporting governance.

TIM is technology independent, so professionals can identify business goals and develop the appropriate architecture for the optimal delivery of data to meet those goals. It uses techniques and terminology that

are largely compatible with current organizational structures and cultures. This highly modular and flexible methodology may be used for projects of varying sizes, scopes, and platforms, especially those involving complex or voluminous enterprise data.

Methodology Phases

HPES supports Agile, iterative, waterfall, and transformational development. TIM is an Agile methodology. Execution of the methodology phases is not sequential; they overlap. Each phase is part of each iteration and increment.

Table 85 highlights the purpose and key benefits of each TIM phase.

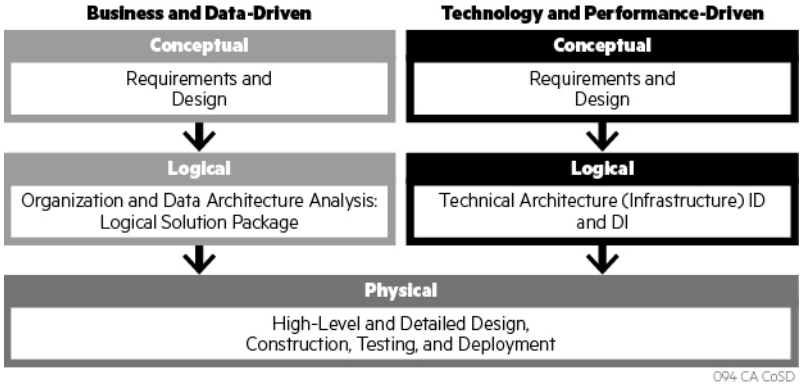
Table 85. Purpose and Key Benefits of each TIM Phase

TIM PHASE	PURPOSE	KEY BENEFITS
Definition	• Clearly define project/program scope. • Complete preparation and planning activities.	Stakeholders' expectations are met.
Requirements	• Elicit, synthesize, and analyze requirements from business stakeholders, data analysis, and information. • Produce clearly articulated, detailed requirements, and business dimensional models aligned to business goals. • Leverage prototypes and perform high-level source data validation.	Requirements are accurate and achievable.
Architecture	• Produce a conceptual-level solution. • Focus on infrastructure architectures. • Apply solution architecture for improved system-wide integration.	Solution architecture integrates all dimensions of the solution.
Analysis	• Establish a vision of work from a data movement perspective. • Define goals in business terms, regardless of technology deployed.	Data movement decisions are made prior to beginning technical design. Implementation is streamlined and resources used efficiently.
Design	• Translate a logical solution into a physical solution. • Focus on high-level/ detailed specifications. • Create detailed design documents.	Solution is project-specific.

We will begin designing the County's transformational solutions at the highest conceptual levels, separating the business solution from the technical solution Figure 169. In this way, the business and data-driven requirements ("what" should be built) are initially separated from technology and performance-driven requirements ("how" it should be built). Separating the "what" from the "how" preempts technologies unnecessarily or prematurely constraining the proposed business solution.

As we progress through increasingly detailed logical levels, we will begin integrating the technical requirements with the business requirements. We will bring in vendor-independent architectural elements, for example, information delivery (ID) and data integration (DI). We will capture the final logical design of the business solution in a Logical Solution Package (LSP), which is the de facto design specification for the physical solution.

Figure 169. Designing Solutions at the Conceptual, Logical, and Physical Levels



TIM minimizes surprises and maximizes business value by delivering high-quality results

- Automated Tools – Automated systems and tools involved in proposed solution

In addition to the tools described above, HPES uses the following tools to support transformational initiatives:

- HPE's Transformational Roadmap (TxRM) - Provides executives with an actionable guide that defines the transformational journey, linking incremental and measurable results to business objectives, priorities, and desired outcomes. It brings clarity to the complexity of transformation.
- HPE's Helion Development Platform - An open, scalable, flexible cloud application platform and ecosystem supporting a variety of runtimes, frameworks, and services. HPE Helion Stack is based on Cloud Foundry® technology, uses Docker containers to launch applications deployed, and offers additional enterprise capabilities for developers and IT operators. HPE's Helion Development Platform is designed to run on many leading Infrastructure-as-a-Service (IaaS) platforms, including AWS, VMware, Azure, and OpenStack.
- This tool supports continuous integration and deployment and helps operations teams deliver cloud-native applications. HPE's Platform-as-a-Service (PaaS) solution enables customers to:
  - Accelerate development of cloud-native applications
  - Reduce cost using a common platform across development and operations.

We are aware that the County needs a full solution to realize the true potential of cloud computing that encompasses both infrastructure services and a robust development platform for developers and applications. Infrastructure-as-a-service is important, but developers also need a fast, easy, and open platform from which to build and deploy applications suitable for the cloud.

- Qualifications and Experience

We have produced TxRMs for many Government clients, including the Department of Homeland Security (DHS), the Internal Revenue Service (IRS), the United States Marine Corps (USMC), the Department of Housing and Urban Development (HUD), and the United Nations (UN). For IRS, we used the TxRM to showcase the dependencies of three domains regarding the future of IT within the IRS enterprise (Infrastructure, Workload, and Data). In doing so, the team was able to expose risks, redundancies, and costs that could greatly limit future success if the requirements were not altered to address ways to mitigate those issues. We obtained agreement across all the IRS' IT lines of business on shared constraints, synergies, and transformational journey.

- Assumptions

None.

- Answers to Specific Questions – Listed below are questions relating to topics of particular interest – if answers are provided already in the context of responses to these Service Framework Components, note in your response with specific cross-references to the questions.

Describe your solution approach to the proposed Transformation requirements.

In the following section, HPES describes our approach to addressing the individual Transformation Projects, as summarized in Table 86.

Table 86. HPES Summary of Answers to Specific Questions (12.1.1 and 12.1.2)

INITIATIVE	PAGE #
Desktop Services (Exhibit KK, Section 3.1)	566
User Data Services (Exhibit KK, Section 3.2)	572
IT Application Portfolio Management Services (Exhibit KK, Section 3.3)	574
Network Transformation (Exhibit KK, Section 3.4)	578
Voice Services Transformation (Exhibit KK, Section 3.5)	585
Storage Architecture (Exhibit KK, Section 3.6)	594
E911 (Exhibit KK, Section 3.7)	608
Identity Federated Services (Exhibit KK, Section 3.8)	610
Other Proposed Initiative (Exhibit KK, Section 4): Enterprise Information Management (EIM)	617
Other Proposed Initiative (Exhibit KK, Section 4): Comprehensive Applications Threat Analysis (CATA) Service	622

Initiatives: Desktop Services (Exhibit KK, Section 3.1)

From our experience working with the County over the past ten years, HPES understands that one of the most pressing IT challenges is meeting existing legacy application requirements. This is in the light of the requirement to transition the County's desktop environment to newer operating systems (e.g. Windows 10) and optimization for current and future technology requirements. It has been a challenge to move to newer operating systems, such as Windows 10, when there are business critical applications which have dependencies on a specific OS, or even a specific browser version and plug-ins.

- Key Considerations and Potential Alternative Approaches

In determining our approach to transform Desktop Services, we considered the following:

- The need to provide the County with innovative methods to more rapidly enable workforce mobility and new styles of IT for their users.
- Decoupling the application from the device, allowing secure legacy application access from anywhere, at any time and from any device
- Decreasing management and support costs by reducing the number of traditional applications on PCs (desktops and laptops)
- Providing the ability to rapidly integrate, provision and leverage new/updated operating systems for end user PCs (desktops and laptops)
- Improving user's productivity and satisfaction by providing improved contextual awareness that is consistent from device to device and compute styles
- Enable a more flexible mobile first, cloud first strategy

We evaluated various approaches that include:

- Desktop rebuild from the ground up
- Desktop Virtualization ("VDI")
- Presentation Virtualization (Application Virtualization)
- Technologies for virtualization from VMware and Citrix

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

HPES proposes implementation of Presentation Virtualization (also known as Application Virtualization) driven by Citrix XenApp. Presentation Virtualization helps address the need by decoupling the legacy applications from the device in such a way that it minimizes the infrastructure and overall costs when compared to other virtualization approaches. In doing this, legacy applications will no longer dictate the upgrade path for the rest of the County's environment and this will minimize the potential for impact if a particular application such as Kronos, Acclaim, or Accela will cause problems with the latest O/S upgrade, or browser version. This, and all of the other virtualized apps, can remain for as long as the County continues to use the apps. Transformation of legacy apps can then proceed on their own timeline, rather than being tied to the remainder of the IT environment.

Each virtualization option, illustrated in the Compute Style section of Figure 170 is generally related to a specific type of user's digital profile, and is typically based on their overall work related IT requirements (e.g. Device(s), Applications, Data, and Support). As the need for more computing power increases (i.e. CPU, Memory, graphics) at the user level, the more complex and costly the virtualization solution becomes.

Project Deliverables:

- Virtualization of up to 200 County applications
  - For up to 15,000 County Users

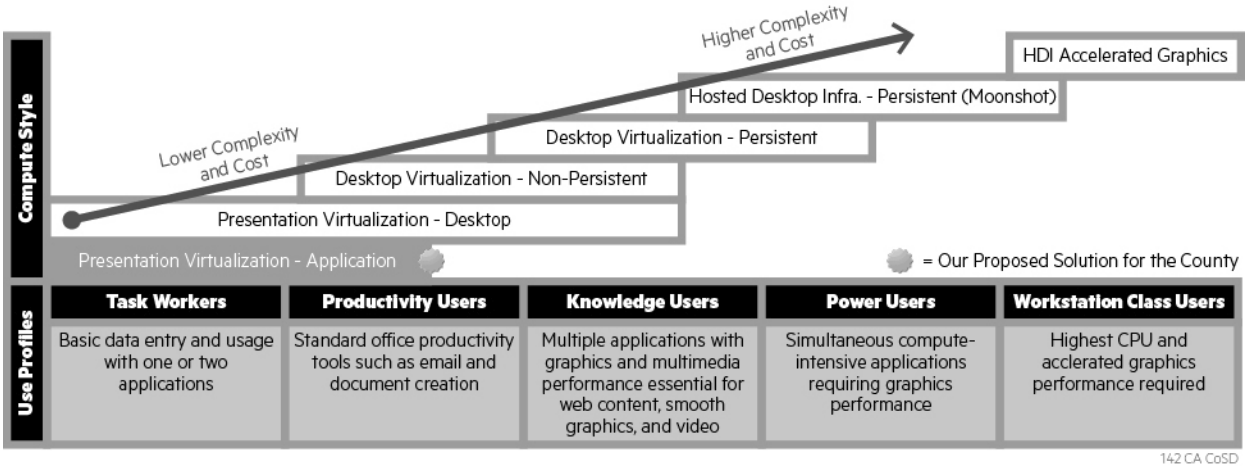
We assume High Concurrency of end users, meaning that for the most part, multiple users will be accessing the application(s) at the same time.

Client virtualization processing load is not only determined by the number of concurrent users, but by the complexity of their applications. The greater the application complexity, the lower the user density per server. As a result, application complexity is an important determinant of the number of concurrent users that can be supported on a given Client Virtualization Service (CVS) solution. HPES classifies application complexity into three groups: light, medium, and complex and has assumed an application profile of medium complexity for the County. Medium Complexity is a standalone application that has minor dependencies on the OS, a prerequisite application, or large/complex data feeds. Most business-related common off-the-shelf applications are considered medium complexity. One notable exception is Microsoft Excel workbooks with embedded macros that can be considered complex in nature.

Specific deliverables include:

- CVS design assessment
- Detailed Presentation Virtualization solution design
- Implementation of the approved solution
- Standardized HPES CVS Presentation Virtualization monthly reports.

Figure 170. Presentation Virtualization



The approach decouples the legacy applications from the device in a way which minimizes the infrastructure and overall costs compared to other virtualization approaches.

Rationale: Presentation Virtualization, provides all the required functionality and is significantly more cost-effective than other solutions, such as VDI (i.e.. Desktop Virtualization, both non-persistent and persistent). We recommend a periodic re-evaluation of Client Virtualization after a number of years, perhaps making the next step to VDI if the requirements change, and if it makes sense financially for the County. This would also be a time to review the current desktop build from the ground up, since VDI would require a much thinner client.

HPES designed the solution for the County to use the same software stack and versions to deploy and to manage it throughout the life of the contract. The solution includes:

- Lakeside Software's SysTrack (for Assessment)
- Citrix: XenApp, XenServer, NetScaler
- Microsoft Server, SQL
- AppSense DesktopNOW Environment Manager.
- Liquidware Labs 'Stratusphere™ UX', Profile Unity and FlexApp
- HPE's Standard Reference Architecture
- Automated Tools – Automated systems and tools involved in proposed solution

Our analysis shows that typically 80 to 90 percent of the use cases can be met by presentation virtualization (typically Citrix XenApp). Presentation virtualization is the most cost effective way to deliver legacy applications when compared to other desktop virtualization technologies, including VMware solutions.

The RFP states that desktop product upgrades or changes to the Applications Portfolio require significant time and engineering efforts to deploy. Presentation virtualization addresses this issue in that upgrade engineering and testing need only focus on one image: that of the server in the data center running the application that is being presented to the user. Virtualizing desktop applications removes a dependency on various desktop client hardware.

This helps prevent deployment delays and post-deployment problems while improving the ability to rapidly maintain desktop currency, at least for the many desktop applications that are virtualized.

Presentation virtualization will also help maximize the performance of all the applications on the end user device, whether virtualized or local.

Timing: The Presentation Virtualization project would follow Transition completion.

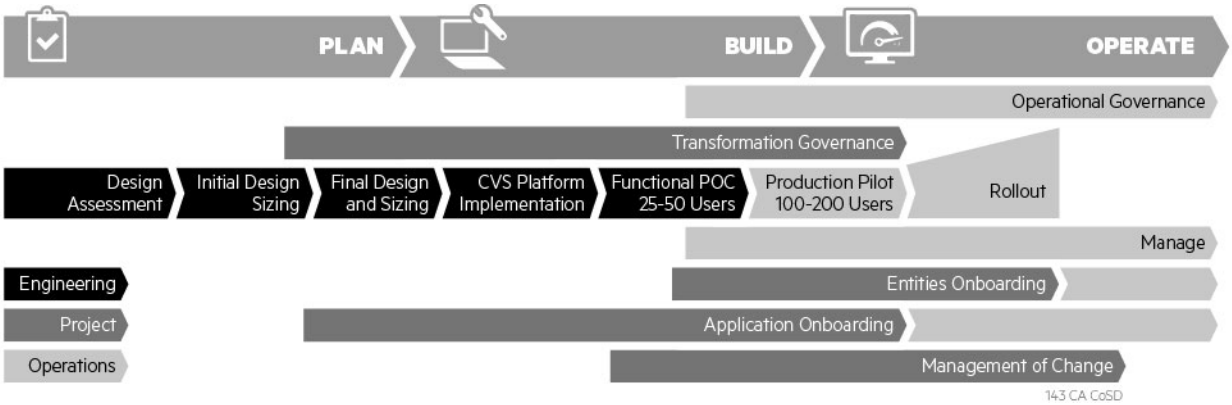
Risk Considerations: The introduction of client virtualization changes the way users perform their work and is therefore considered disruptive. Failed first attempts to introduce users to client virtualization result in roll-out delays, onboarding program rework and reintroduction to users which is costly, time consuming and can significantly erode the expected ROI. For a high degree of success, consider the following:

- **Entity onboarding** - Depending on the structure of the customer and according to the priorities defined during the assessment/analysis/design phase, we recommend ramping up users by personas (groups of users). User personas could be a business unit, a department, a typical group of user profiles based on common desktop or application requirements. This will involve identifying people, managing the persona grouping, desktop and application group entitlements and orchestrating this by means of Active Directory.
- **User onboarding** - Onboarding management and Client Virtualization Service (CVS) Management links the two onboarding subphases (Entity and User onboarding). We propose to migrate a category of virtualized users either by a specific persona and/or with relatively similar desktop/application requirements, and begin with less complex use cases then progress to the more complex. Subsequently, the scope will be increased until all users have been on boarded successfully.

All onboarding activities are managed and controlled by an onboarding manager. Once users are successfully onboard in the production environment, they are managed like any other user with a CVS Service Manager. The CVS Service Manager monitors the overall performance of the virtualization service, coordinating performance review meetings and reports with both the customer and CVS operations.

Key dependencies and Milestones: Our proposed deployment is comprised of two discrete parts, with the second part dependent upon completion of the first. These are CVS design assessment and implementation.

Figure 171**. Representative Key Milestones for a Presentation Virtualization Deployment**



Please note that the durations and dates of the major tasks are dependent upon the data gathered from the first step, the Design Assessment. After the Design Assessment, HPES develops the final implementation timeline. Typical Presentation Virtualization projects of similar complexity to the County's take approximately five months.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The following HPES resources will support this transformation project:

- The HPES Workplace Transformation Consulting Team will perform the CV Assessment
- The HPES implementation team consists of
  - An overall Program Lead that is a subject matter expert (SME) in End-User Compute solutions.
  - Additional SMEs based on the overall solution scope and may include but is not limited to: project management, deployment and implementation planning, infrastructure specialists, user onboarding, training, Image Creation / Mgmt., application packaging and testing.
- A senior Transformation Manager who is responsible for the end-to-end project scope and stays in place until acceptance criteria have been met.
- Ongoing support for the Presentation Virtualization service will be delivered by US-based delivery resources in line with the County's requirements.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

We follow a proven methodology for CVS implementation that begins with the CVS Design Assessment, and continues through implementation and ongoing management as described below.

CVS Design Assessment: HPES will assess a sample of existing County users, looking at how they interact with their apps and analyze how the apps interact with users' devices. This helps the appropriate applications for each user type to be identified and drive the transition plan from the current mode of operation (CMO) to the desired future mode of operation (FMO). This assessment will take into consideration the following items:

- The desktops included will be a sample of end-user desktops for each type of user and IT usage
- A "Type of user" categorization, which refers to the type of applications users work with the intensity with which they use them as measured by CPU, RAM, disk IO, and network traffic
- A "Type of usage" categorization, which includes not only the PC, laptop, tablet, smartphone, or engineering workstation each user needs to do his/her job, but also any requirements for peripherals such as USB connected security dongles, portable data storage, cameras, meters, and other specialized devices. The goal is to identify the subset of IT usage that provides the majority of business value, identify a solution that meets the core requirements for providing that business value, and, after the core requirements are met, identify how to support all other candidates for virtualization for the optimum incremental cost.

There are three steps to the Design Assessment:

- Startup
  - Developing a statement of requirements to confirm that the engagement team understands the purpose of this engagement from the County's point-of-view
  - Developing a data collection plan that details how the engagement will collect the data needed for this assessment: The purpose of this plan is to enable County personnel responsible for change management and information security to approve the data collection.
- Execution
  - Meeting notes from a discussion of the County's intended future mode of operation (FMO) to confirm that engagement team understands the desired outcome
  - An assessment report that summarizes and analyzes the collected data: The engagement team will review this assessment with County stakeholders
- Closedown
  - A solution document that identifies the next steps that the County and engagement team have jointly recommended as a result of reviewing the assessment report.

This assessment validates the initial assumptions or identifies necessary modifications of the initial assumptions related to the original scope for this effort. This revised scope, based on the data that was

gathered and analyzed, can affect the original solution and can have an impact on the overall solution components including; infrastructure, labor and software that is required for the solution.

CVS Implementation: At the start of the implementation phase of the project, we hold a workshop to begin the planning process. We will work collaboratively with the County to identify and agree upon key milestones and objectives, and we will report status on these throughout the implementation.

We have an established and proven transformation methodology that follows an industrialized "factory" approach. This methodology is organized in phases, as described in the following overview, with clear milestones that are established by HPES and the County after the Design Assessment. We then create a mutually agreed to transition plan with a detailed work breakdown structure, milestones and owners for execution.

The activities executed during the Implementation Phase of the project are:

- Design Sizing (Initial, Final)
  - Review of assessment data (user usage, application usage, network, user data, security)
  - Architecture Design and Infrastructure Implementation Plan established
- Infrastructure Set-up
  - Site preparation in the Tulsa data center and equipment provisioning. This environment can be implemented as an expansion to your MPC environment, or as a standalone virtual infrastructure under the HMCB, in order to integrate it with your hybrid cloud.
  - Server installation (HW and operating system)
  - Server integration in the County's Active Directory Domain
  - Server integration in the Tulsa data center and linkage to other infrastructure service (DNS, Storage, proxy, AV system, etc.)
  - Software implementation and configuration
- Functional Testing
  - Functional pilot or Proof of Concept (POC), is performed by a small group of IT users to verify compliance (to functional and technical requirements) and performance of the solution, and tune the configuration if necessary.
- Production Pilot
  - While the functional testing above is focused on IT users with client virtualization familiarity, this testing phase focuses on the general user population with the goal of testing both the technical solution and the roll-out plans and materials.
  - The Production pilot is performed with 100 to 200 selected users operating in the production environment. This pilot is for a fixed, short period of time. Test scripts are supplied to pilot users that identify the specific activities a participant should perform. We then examine the results for faults and provide feedback to the delivery team. We correct any faults, either by correcting the script, user performance of the script or infrastructure/software correction. Once corrections are in place, we re-run the script will be re-run until all test scripts are successfully completed with no issues.
- Onboarding
  - During this phase, we manage two kinds of onboarding (Entity and User, as mentioned above), each of which potentially influence the other. Workgroup/departmental similarity in application use, security, and the County's implementation priorities are the main factors in identifying a roll-out plan.
- Management of Change
  - Throughout the entire pilot and rollout period, the Transformation Manager will work with the implementation team and the operational support team to verify that the rollout plans are communicated, support is in place and end user issues are addressed.

- Qualifications and Experience – Background and experience in comparable environments

HPES has demonstrated extensive industry knowledge and experience managing virtualized computing environments, with more than 725,000 seats deployed. Based on the most recent version of The Forrester Wave™ for Global Workplace Services HPES is positioned as a Leader.

We leverage our relationships with market leaders—Microsoft, Citrix, and Liquidware Labs—to create a fully integrated client virtualization solution that provides better security, greater flexibility, and lower costs than locally installed applications or desktops on traditional PCs.

> "A client virtualization implementation requires software, hardware, and services and a proven methodology to enable faster installation of the right solution the first time. HPES is one of the few companies that can offer all of these components."
>
> *IDC white paper; Driving business Value With Virtualization*

Our experience and expertise includes:

- Reachback to highly qualified delivery personnel in Centers of Excellence around the world to take advantage of the knowledge gained from previous client engagements. With more than 300 Citrix Certified professionals, HPES has the experience to deliver even the most complex solutions. We are currently managing 725,000 virtualization seats and 100,000 virtual applications in almost every industry.
- Serving more than 570 clients in 135 countries
- More than 15 years of experience providing Client Virtualization Services
- Recognition as a VDI market leader and innovator with over 650K (and growing) seats deployed in in multiple industries and countries - Nelson-Hall
- Using market-leading technology from Citrix, Liquidware, and Microsoft delivered through a global center of expertise and four global delivery locations

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

Initiatives: User Data Services (Exhibit KK, Section 3.2)

- Key Considerations and Potential Alternative Approaches

One of the steps to achieving a truly mobile workforce is to separate the data from the device. By doing so, County employees will be able to access the data necessary for their job from any number of devices, whether County-owned or through Bring Your Own Device (BYOD), or even via the Web. Knowing this, we have formulated a number of key considerations. The solution must have the following characteristics:

- Be secure
- Allow user data to be decoupled from the user's device
- Take advantage of existing licensed solutions, tools, and services
- Allow various levels of access.
- Support collaboration both within the organization and external to it.
- Finally, County users span many different types of work, and they are multi-generational as well. Because of this, our solution balances a new way of interacting with one's data along with the need to maintain some form of familiarity.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

HPES recommends taking full advantage of the technology the County already has using your Office 365 subscription and OneDrive for Business. This solution satisfies the specific requirements of the County identified in Schedule KK, Section 3.2, and it addresses a multitude of possible Use Cases.

OneDrive for Business includes apps for smartphones, and allows mobile access through the mobile device management (MDM) solution.

As subscribers to the G3 level of Office 365, each user has 1TB of space on their OneDrive for Business account. Microsoft research shows that the vast majority of business users consume much less than 1TB our research on the County's historical use of file shares supports this. The entire size of County network shares is 78TB for all 15,000 users. HPES will continue to work with Microsoft to facilitate optimal configurations.

End users can collaborate in several ways. Using OneDrive for Business, a user can share a document or series of documents from their own OneDrive for Business data space. The documents themselves are not delivered to the other user. Rather, a link to that document allows the designated user (and no one else, besides the owner) access to only the documents the owner wants to share.

Departments or divisions that want to have a shared space for their exclusive use can create "groups." Access to these groups is initially fully locked down. The owner of the group would have to explicitly invite members to use the shared space.

To fully realize the benefits of Office 365, users must make the move from using network file shares to storing their data on OneDrive for Business. We propose a project to migrate data on user network file shares to their OneDrive for Business location. The project steps at a high-level are:

- **Group Policies / Powershell Scripting.** The moves will be automated via Powershell scripts and actioned via group policies.
- **Search for invalid files/folders and cleanup.** OneDrive for Business has different requirements for filenames and folder structures than Windows. We will need to locate the files that will not move in their original states.
- **Pilot.** We will migrate a test group of users via automated processes.
- **Scheduling.** The migration will need to occur in waves. The project plan assumes a conservatively low size of 300 users per wave. As the waves progress, the size of subsequent waves might grow, thereby shortening the project.
- **Communication / Training.** OneDrive for Business is a paradigm shift from the traditional way of interacting with data files. We will develop and deliver a communication plan as well as training for users who migrate to OneDrive .
- **Migration (waves).** The migration will occur in waves, with support throughout the entire project. At the end of the project, all County users will have completed a migration from a network share data to their OneDrive for Business account.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

For OneDrive for Business, all data is stored in Microsoft's Government Community Cloud.

Support for OneDrive for Business will come from the Service Desk. OneDrive for Business issues will take advantage of our enhanced support for Office 365 service, which uses HPES support resources working on-site with Microsoft Office 365 support engineers.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

We support OneDrive for Business, using time-tested infrastructure processes of both HPE and Microsoft, which emphasize delivering measurable, repeatable, and efficient services to the end user.

- Automated Tools – Automated systems and tools involved in proposed solution

For the rollout and subsequent maintenance of the end-user device connectivity to OneDrive for Business, we will use Group Policy through Microsoft System Center Configuration Manager (SCCM). This will allow a smooth rollout of the solution and will make subsequent revisions for new requirements easier as well.

- Qualifications and Experience – Background and experience in comparable environments

Internally, HPES has transitioned ~300,000 users (HPE/HPI combined) to OneDrive for Business, using it for individual storage, collaboration, sharing, and device backup. HPES will follow a similar process to successfully migrate the County to the OneDrive for Business solution.

This solution takes advantage of our 30-year history of partnership and collaboration where HPES is the only Microsoft partner to have co-located shared support resources for Office 365 for the exclusive use of our customers.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

Initiatives: IT Application Portfolio Management Services (Exhibit KK, Section 3.3)

- Key Considerations and Potential Alternative Approaches

Over the past 10 years, the HPES account team has developed a proven practice to manage the County's IT application portfolio. The foundation of this approach is close collaboration with County stakeholders, GITMs and department leads, plus incorporating numerous tools to gain access and visibility into applications usage, usefulness and life. Ongoing application rationalization has helped facilitate this decision making by looking at gaps, and reducing complexities surrounding the application portfolio. It has also helped to support new business initiatives by providing information that links strategy to intelligent investments. Our application rationalization project in 2012 led to a number of major projects that have benefitted the County, such as

- Replacement of a third party eBenefits system by incorporating its capabilities into a Peoplesoft upgrade
- Implementation of iTrack as collection point and system of record for Information Technology Outsourcing (ITO) expenditures
- Deployment of the new Electronic Document Processing Platform (EDPP)

IT Application Portfolio Management supports the continuous assessment of IT application portfolios to:

- Standardize portfolio management
- Align the IT application portfolio with business strategies
- Reduce deployment time
- Improve operational efficiencies
- Reduce costs and optimize value
- Increase visibility and understanding of the application portfolio

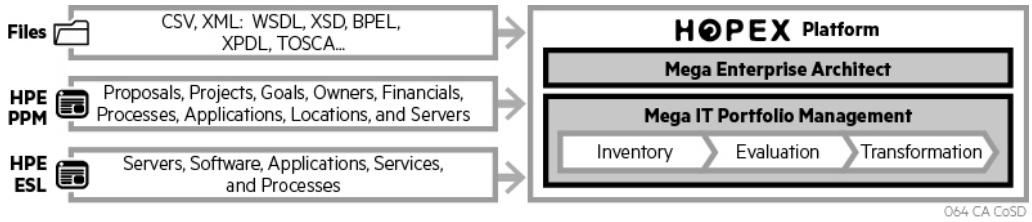
Key considerations for this transformation project require selecting a tool suitable for meeting the criteria listed below. These criteria are based on the initial list of items contained in Exhibit KK, and derived from the requirements.

- Highly configurable
- Integrated environment
- Integration with source systems
- Speed of implementation
- Develop architecture disciplines to maximize in-place tools
- Business capability mapping
- Incorporation of application portfolio inventory
- Define cost elements
- Project-related information
- Rationalization alternatives/recommendations

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution: MEGA's HOPEX platform offers a comprehensive, well-rounded, feature-rich platform that provides an out-of-the-box metamodel that is highly configurable and has strong modeling capabilities. It also supports a wide range of industry frameworks. HOPEX combines industry-leading practices in enterprise architecture (EA), IT portfolio management (ITPM), business process analysis (BPA), and governance, risk, and compliance (GRC) into a single platform. This integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation as shown in Figure 172.

Figure 172. MEGA IT Portfolio Management



This fully integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation.

Use of this tool facilitates creation of a complete inventory of IT assets, including applications, underlying technologies, and servers. Both out-of-the-box and custom reports provide information that makes it easy to evaluate IT assets using multi-criteria analysis such as costs, risks, technical efficiency, and business value, bringing visibility to the County's IT portfolio. This information also provides insight about dependencies and helps to identify redundancies of IT systems while reducing costs and complexity by eliminating systems with the same functionality. MEGA also provides the ability to create and compare multiple transformation scenarios that take into account various criteria to select the most relevant scenario for their business needs and constraints.

Upon approval from the County to proceed with this transformation project, HPES and MEGA consultants will schedule a project planning and kickoff meeting. A topic of discussion for this meeting will be identification of County stakeholders that requested to participate in requirements gathering sessions to make certain the MEGA ITPM is configured correctly to meet the requirements.

Once in place, MEGA ITPM provides a three-step approach to managing IT assets:

1. **Inventory**: ITPM automates the collection of IT assets through a web-based interface. It provides metadata that can describe IT assets through various parameters such as functional scope, lifecycle, costs, and risks, providing a comprehensive view of the existing IT portfolio.

The inventory creation will use MEGA's APIs to interface with the ESL, partner systems, and other feeder systems (i.e., AppsManager) to make certain accurate data is in place. Once the inventory data is populated, IT assets can be viewed by business lines, business processes, business capabilities, organizational units, and technology vendors.

2. **Evaluation**: This step assesses IT assets through either out-of-the-box or custom criteria such as costs, risks, business value, and functional support. It provides detailed analysis through cost, dependency, and impact reports (i.e., Brick's compliance). To rationalize the portfolio, it provides insight into which IT assets need to be removed, replaced, or maintained. Using business capability maps, IT assets are organized by functional areas, and changes are displayed over time, helping to make better-informed decisions.

Also during this step, costs and other project-related information are associated with the assets. The IT assets are evaluated by business value, functional support, and technical efficiency through the use of IT portfolio evaluation campaigns.

3. **Transformation**: In this step, the County can define a mix of initiatives or assumptions such as extending, replacing, or phasing out applications and technologies and compile them into different scenarios. The County can then assess and compare these scenarios through various criteria such as risk to quality, risk to feasibility, and costs and then identify the best transformation scenario to implement.

Rationale: The County has stated a clear preference for the MEGA ITPM tool. We have designed this project based on the recommendations of the product supplier, with the following characteristics and caveats:

- As requirements evolve, additional MEGA modules, such as Enterprise Architecture and Governance, may be required.
- Information from the HPES ESL, PPM, and AppsManager will be maintained by the source systems and will be updated by MEGA at scheduled times.
- MEGA out-of-the box functionality will be used for this effort.
- HPES will install, configure, and manage MEGA modules.
- Licenses are included for MEGA HOPEX WorkBench and ITPM module for 30 contributors, 10 Portfolio Managers (GITMs) and 5 Advanced Users (CTO).

Timing: HPES proposes to use the MEGA Quick Start program for implementation of MEGA ITPM. In the MEGA Quick Start program, HPES will collaborate with MEGA consultants to conduct a project kickoff that includes the definition of project scope and schedule. Typical installation and configuration of a MEGA project takes about 45 days, including installing and configuring MEGA ITPM, conducting functional/deployment specifications workshops, designing supporting MEGA metamodels, testing the changes, reviewing and mapping the artifacts, uploading the artifacts, establishing portfolios and hierarchies, and training supervisors and users.

Risk considerations: Potential risks that could affect the project include the following:

- Automating APIs and metamodels will require configuration and potential connector development to accommodate integration with external systems of record: AppsManager, PPM, and HPE's ESL.

Key Dependencies and Milestones: Following are the key milestones and dependencies for the project:

- Kickoff: Receipt of County approval to begin will initiate kickoff of the engagement. After the kickoff session, we will define the project scope and develop the schedule.
- Installation: The next milestone is installation of MEGA on the established infrastructure. This is dependent on the availability of SQL Server licenses and availability of the infrastructure.
- Specification: The next milestone is conducting and delivering the functional/deployment specifications workshop. Part of this deliverable will be demonstration of MEGA ITPM capabilities. HPES will prepare an ITPM customer guide. The deliverable will include the functional/deployment specifications and customer guide. This task is dependent on availability of the designated County users who will provide the requirements for use of the MEGA system.
- Configuration: The next milestone is reached when the configuration and customization of MEGA is completed using the functional/deployment specification as defined above. During this step, the supporting MEGA metamodels will be designed, built, tested, and implemented.
- Artifacts: The next milestone is reached when all artifacts are uploaded in MEGA after reviewing and mapping the ITPM specific artifacts. The portfolios and hierarchies will also be established during this cycle. At this time we perform acceptance testing to verify that it is set up correctly.
- Training: This milestone will be followed by a training session for users.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Resources: For implementation of the MEGA ITPM toolset, HPES will use MEGA's Quick Start program. MEGA's experienced consultants will work with us to install, configure, and set up the MEGA environment. MEGA consultants and HPES staff will work with County staff to demonstrate MEGA HOPEX functionality, determine functional and deployment needs, and document the supporting requirements. To minimize the County's time investment while maximizing impact, we will conduct information gathering workshops through a series of focused discussions with stakeholders to make certain that we have an accurate understanding of the County's needs. At the end of this effort, we will deliver a functional deployment specification and a user guide. We will then help design MEGA metamodels and make the configuration changes to interface with PPM, ESL and AppsManager systems. We will then upload the artifacts and establish portfolios and hierarchies in accordance with the County's needs. Our team will also provide training for the user groups who will use MEGA ITPM toolset.

The HPES team supporting the MEGA toolset will work closely with CTO, and supporting staff to provide a collaborative working environment. This will enable direct communication and provide the County with the ability to reach out directly to HPES personnel for quick resolution of any issues.

Facility: HPES will locate the MEGA infrastructure in the Tulsa data center.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

We will perform the installation, configuration, and management of the MEGA ITPM toolset using ITIL v3 processes, consistent with the established processes for managing County assets. We will use our system development life cycle (SDLC) processes in collaboration with the County staff to configure and make necessary updates to MEGA application programming interfaces (APIs) to align with automated systems and tools involved in proposed solution

The MEGA ITPM tool provides all required functionality to meet the County's requirements, and it will integrate with AppsManager, PPM and the ESL solution.

- Qualifications and Experience – Background and experience in comparable environments

HPES manages COTS product implementations across many Federal and state agencies and uses the MEGA toolset at Procter & Gamble (P&G). At P&G, we deployed and configured the MEGA Suite as the company's system of record for business, information, application, and technology architectures. The suite was designed to let P&G map out and understand processes and how they relate to the services that it delivers. The suite is integrated with the P&G service management stack to integrate portfolio artifacts. HPES provides advisory services to help P&G identify and eliminate redundancies and gaps. Through this process, P&G expects to be able to develop and deliver these shared services at lower cost, resulting in financial savings for the company. The MEGA Suite has become the system of record for all architectures: business, information, application, and technology. It is one of the core systems for the IT landscape on which P&G runs shared services for the company. The MEGA Suite allows information to be changed once in the repository; the updated data flows across the IT landscape.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

- None.

Initiative: Network Transformation (Exhibit KK, Section 3.4)

- Key Considerations and Potential Alternative Approaches

The HPES network team has implemented a unique approach to transformation that has set a new standard in its effectiveness and ability to align with County strategy while delivering vision and perspective that enable the evaluation of near-term and long-term opportunities. The foundation of this approach is close collaboration with the County Technology Office (CTO), the HPES Chief Technical Architect, and the HPES Enterprise Architecture team. Technical leadership meet weekly to discuss strategic objectives and the technology and industry influences that provide the impetus for new solution development.

Our team has adopted a "start fast" approach that enables experimental and rapid evaluation of technology—many times in the production environment—that helps our teams understand not just the viability of a potential solution but the integration challenges associated with it, including those that could impact adjacent frameworks. This bi-modal "mode 2" approach has proven extremely effective in driving continual improvement across the entire enterprise. As new solutions to business problems are evaluated, this iterative practice makes certain that our roadmaps remain agile—not bogged down with dependencies—with traditional planning efforts saved for solutions already confirmed as viable.

We save time, drive change rapidly, and identify fatal flaws before solutions are brought into the environment, in turn avoiding costly overruns and business impacts. We are proud of this approach and believe that ultimately it will continue to position the County as a leader in its utilization of IT as an enabler to the enterprise.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

The HPES approach to network transformation leverages the existing investment that the County has made in its infrastructure, building on the robust, geo-redundant network core to enable new service adoption while we migrate from legacy technology. This foundation positions the County to make smart, progressive choices in the way services are delivered to its employees and constituents, regardless of their location or access device. As the County network continues to evolve, our ability to provide ubiquitous connectivity with seamless accessibility, security, and performance will provide the benchmark of our framework.

The solutions highlighted in this section include transformation initiatives planned for implementation early in the term as well evolutionary technologies that may arise later in the contract life cycle. In the near term, all defined solutions represent planned implementations inherent to the services described in Section 4.3 of the RFP and are priced in Schedule 16.1-1 accordingly. Relative to statements focused on technology not yet available for deployment, AT&T will evaluate the feasibility of these solutions and provide roadmaps over the contract life cycle. If identified as a viable replacement to existing services, AT&T will make recommendations for upgrades in line with refresh obligations or as otherwise agreed to with the County.

Cloud Enablement via NetBond

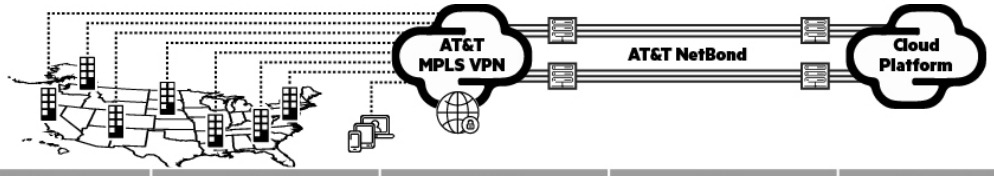
As cloud-based services mature and become more viable for Government use, we are positioning the County's network perimeter to enable seamless, secure, and performance-assured integration for cloud providers. AT&T will build a geo-redundant core network foundation to enable this shift in services, leveraging AT&T's virtual private network (AVPN) MPLS-based transport. This foundation will be deployed as a transformation activity in preparation for future services early in the contract term and is priced in Schedule 16.1.1.

Building on our AVPN transport, AT&T's optional NetBond service will be made available on a per cloud provider basis, enabling secure, performance-assured cloud-to-enterprise peering, in turn isolating these important services away from the unsecure and potentially congestion-prone Internet Service Provider (ISP) links. The NetBond service is represented in Exhibit 16.1.2 as a proposed new RU, where the County can select peering relationships with designated cloud providers on a bandwidth scaling basis. Cloud provider side costs may apply and will be priced as new RUs when establishing a new cloud provider contract, as requested by the County.

In support of the transition of Exchange to the O365 cloud, AT&T offers the optional service that will enable Netbond functionality in a peering arrangement with Microsoft's ExpressRoute product. This option will be designed and implemented in line with the specified transition plan and is priced as a separate resource unit that combines the NetBond RU (highlighted in Exhibit 16.1.2) with the ExpressRoute costs to complete the connectivity model for the service.

Figure 173 illustrates NetBond benefits; Figure 174 represents some of the well-known cloud services partners to which AT&T currently supports connectivity via NetBond; Figure 175 depicts security benefits of AT&T NetBond; and Figure 176 shows the performance benefits of NetBond.

Figure 173. AT&T NetBond Benefits



Performance	Security	Simple	Agile	Cost Effective
Direct on-net routing; reliable redundancy	Separates customer data; flows to the cloud	Easy to add and change cloud access in near-real time with API	Built-in "burstability" that scales in tandem with cloud	Cloud-like pricing with no long-term commitments

025 CA CoSD

Figure 174. Well-known cloud services partners that AT&T currently supports via NetBond.

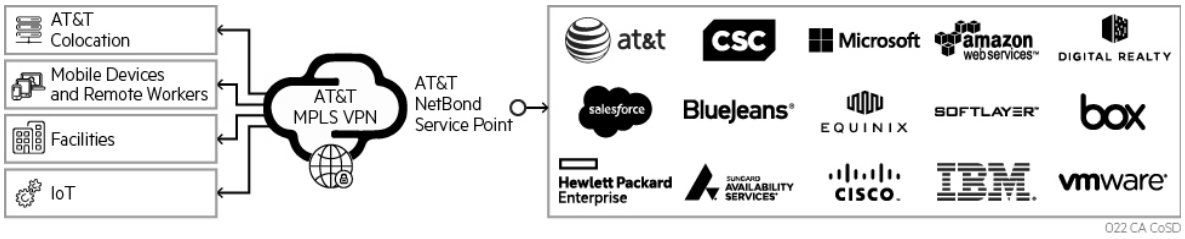


Figure 175. Security Benefits of AT&T NetBond

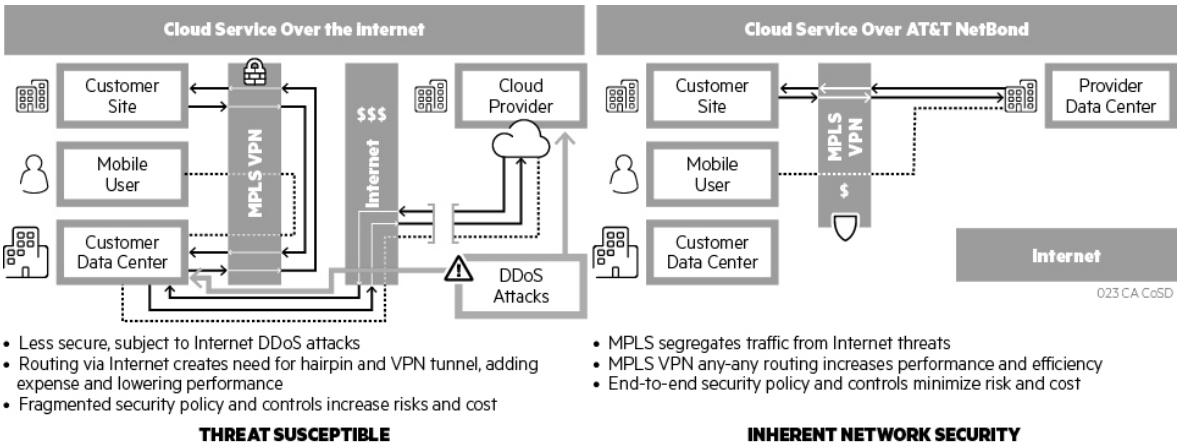
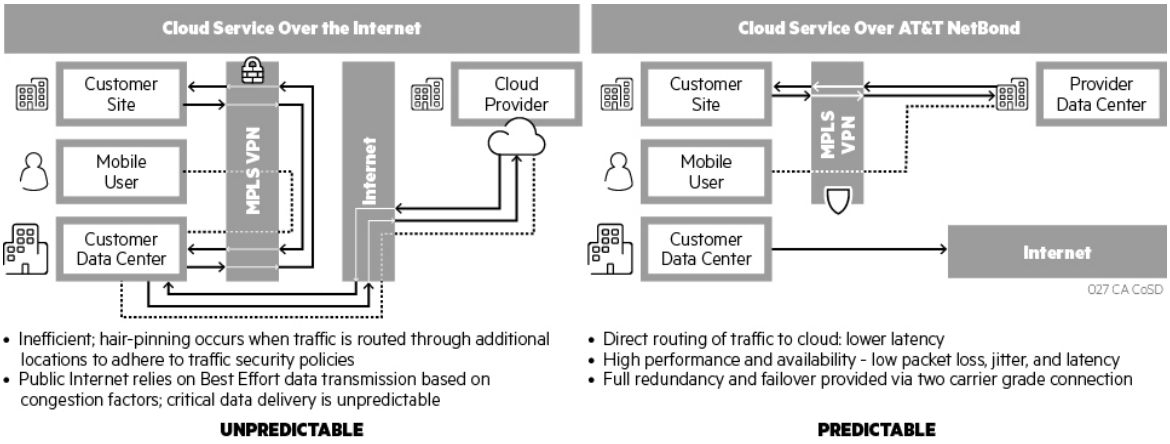


Figure 176. Performance Benefits of AT&T NetBond



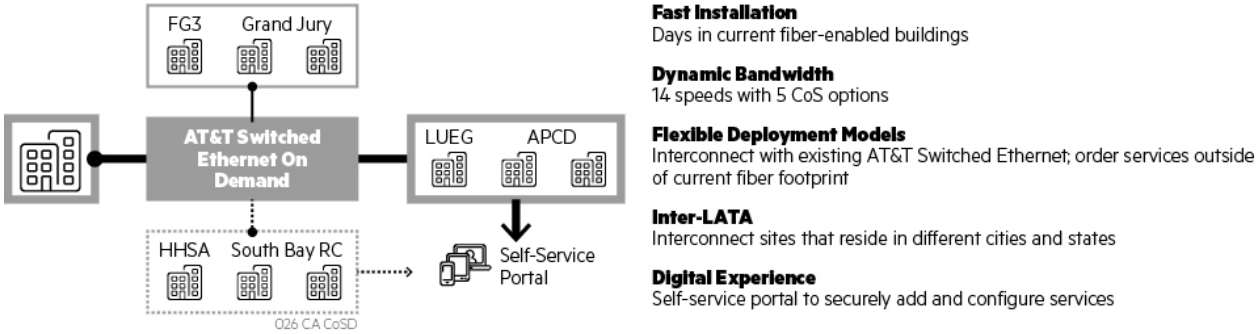
Migration to AT&T Switched Ethernet with Network on Demand

HPES' transformation plan for the County's wide area network (WAN) includes migration of all 115 OPT-E-MAN Metro Ethernet connected sites to the AT&T Switched Ethernet with Network on Demand (ASE w/NOD). Additionally, all data T1 sites will be evaluated for migration and where available without significant special construction costs, sites will be migrated to this new service. Special construction costs apply when fiber based transport is unavailable in the "last mile" from an underground or above ground exchange nearby a given site. The fiber install from these local exchanges is included in normal construction, but installing extended runs to new areas with no local exchange would be grounds for special construction. During the design and provisioning process, HPES will provide a list of T1 sites to

the County with special construction costs for consideration. At the time of this proposal, it is believed that 80-90% of the existing T1 sites are eligible for migration to this new service.

Using software defined networking (SDN) capabilities inherent to ASE w/NOD, bandwidth can be adjusted within 15 minutes from as low as 2 MB to as high as 1 GB. Coupled with real-time capacity management capabilities, this new service will allow rapid response to County bandwidth needs as well as enable the planning of additional throughput for scheduled events. Additionally, the deployment of fiber-based services will further improve consistency, availability, and performance of the remote sites across the network. Figure 177 lists benefits of AT&T Switched Ethernet On-Demand Service.

Figure 177. AT&T Switched Ethernet On-Demand Service Benefits



ASE w/ NoD Site Redundancy

HPES has evaluated enabling additional remote site redundancy at key County facilities. The facilities listed below are historically some of the most important to County business functions and are the recommended sites for this enhanced service. It's important to note that the site list includes two sites that are currently on the Gigabit backbone (Sites 18 & 33), but are planned for migration to ASE w/ Network on Demand as a part of the Network Transformation, Backbone Consolidation project (see next section).

Site #	Site Name	Street Address	City	Zip Code
13	Children's Service Center (Adoptions Center)	6950 Levant St.	San Diego	92111
18	MTS Trolley Tower (Mills Building)	1255 Imperial Ave.	San Diego	92113
19	Lemon Grove District Office / FRC	7065 Broadway	Lemon Grove	91945
33	Health Services Complex	3851 Rosecrans St.	San Diego	92110
35	Animal Control-Central Shelter	5480 Gaines St.	San Diego	92110
55	Oceanside Service Center	1315 Union Plaza Ct.	Oceanside	92054
56	A. B & Jessie Polinsky Children's Center	9400 Ruffin Ct.	San Diego	92123
57	Child Welfare Services - Central	4990 Viewridge Ave.	San Diego	92123
80	Assessor/Recorder/Clerk Kearny Mesa	9225 Clairemont Mesa Blvd.	San Diego	92123
81	Assessor/Recorder/Clerk San Marcos	141 E. Carmel St., Bldg. 1	San Marcos	92078
95	HHSA FRC Center South Bay	401 Mile of Cars	National City	91950
190	HHSA FRC Center Escondido	649 W. Mission Ave.	Escondido	92025
205	Edgemoor Geriatric Hospital	655 Park Center Dr.	Santee	92071
260	Assessor's Revenue and Recovery	590 3rd Ave.	Chula Vista	91910
290	Access 211	8765 Fletcher Pkwy.	La Mesa	91942

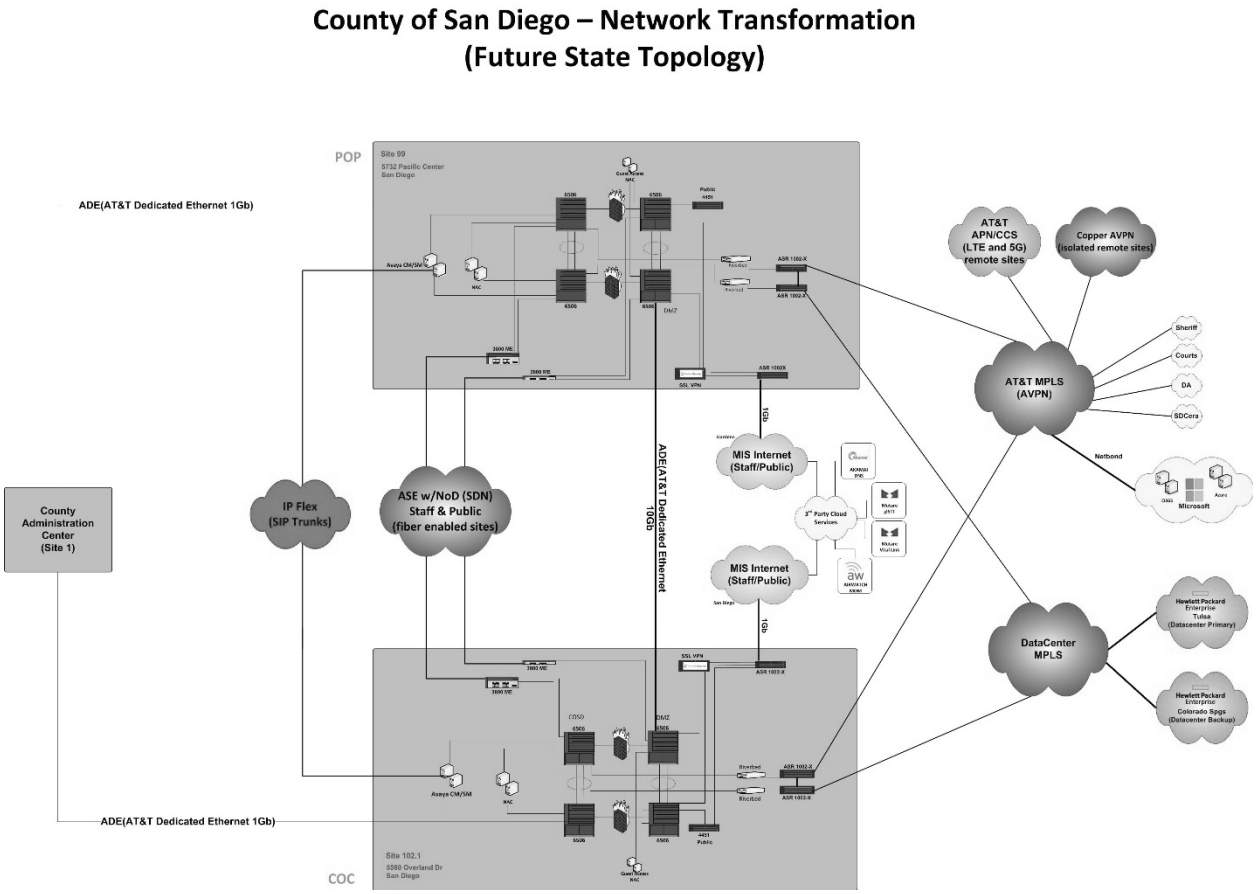
The standard Network on Demand design provides geo-redundant host circuits, however from the last Central Office, this diversity is reduced to a single fiber pathway to the remote site. The redundancy design will involve provisioning a redundant circuit with diverse fiber path and infrastructure from an alternate central office. This secondary pathway will extend to the remote site, entering via redundant entrance facilities. The circuits will be ordered and built as stand-alone circuits and configured with minimal bandwidth, which will leverage the Network on Demand near real time bandwidth provisioning capability to provide fully functional bandwidth in the event of a failure on the primary path.

HPES proposes the completion of requisite core transport design work which will result in a per site construction cost for County consideration. This process will also allow the County to evaluate cost of diverse entrance facilities. These one-time costs would be the responsibility of the County. The County may evaluate these costs and select sites that have the greatest benefit without being cost prohibitive. As these sites are selected, and one-time costs agreed, HPES will execute an order for the service. This offer will remain valid over the first four (4) years of the contract term. County requests to add sites not listed in this proposal will be handled on a case by case basis.

Backbone Consolidation

AT&T also adheres to the concept of keeping it simple where possible. While some network solutions can be incredibly complex, the core architecture does not have to be. By reducing the number of core backbone sites (GigaMAN Connected), AT&T can simplify the network architecture while providing redundancy, sufficient bandwidth, and throughput for County business. This allows us to right-size and tailor services in accordance with the needs of a location without the costs, equipment, and infrastructure inefficiencies that come with unnecessary capacity. The net result is standardization of transport connectivity across all County sites, providing the shortest path to services, in turn leading to predictable performance, improved security, reduced maintenance cost, and lower mean time to recovery (MTTR) in the event of an incident. Figure 178 illustrates the future-state network topology.

Figure 178. County of San Diego Network Transformation (Future State Topology)



Session Initiation Protocol (SIP) Core Expansion

Our network team has already begun the process of transformation within the County to phase out Time Division Multiplexing (TDMbased voice connectivity in favor of Session Initiation Protocol (SIP)-based solutions. Our SIP infrastructure is provided via two AT&T IP flex trunks, provisioned over the geo-redundant AVPN core network, that are dynamically available and sized to take a full production load of traffic in the event of a circuit failure. Currently, the SIP trunks are configured to support local outbound calling. Expanding on this foundation, we plan to increase the capacity of these trunks to enable support of all Avaya core network controlled outbound calls, including local, long distance, and toll services. This expansion will eliminate outbound usage-based costs for these legacy resources units. Inbound calls will be migrated to SIP including Toll Free 800 services, which will substantially reduce the usage charges associated with Toll Free 800 services. Over the life of the proposed contract, we will continually evaluate the capabilities of these trunks to support additional voice and unified communication services.

Future T1 Migration for Non-ASE with Network on Demand Sites

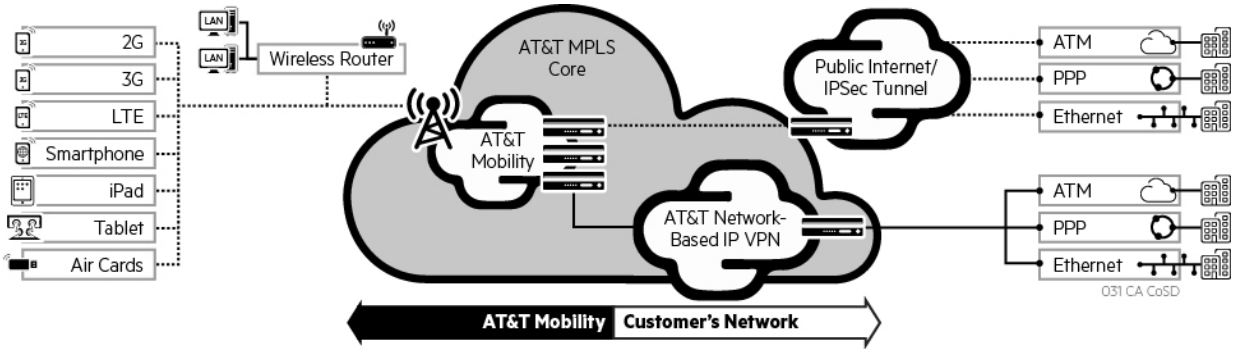
As identified earlier, T1 transport utilizing legacy TDM based connectivity, will be targeted for migration to ASE with NOD where possible. However, where fiber is not available without prohibitive construction cost, AT&T will evaluate products such as copper-based AVPN that provides transport redundancy to the geo-redundant core. This service layers an AVPN service over a T1 copper circuit, providing AVPN cloud connectivity from a central office, creating pathway redundancy across the LAN. This solution continues to leverage the copper based wireline infrastructure that supports the site today, with a single

point of failure still remaining on the "last mile" of transport to the remote site. As we evaluate our options for eliminating T1 sites these factors may drive us to pursue other alternatives.

Such an alternative could leverage the AT&T mobility network infrastructure using Commercial Connectivity Services (CCS) over a private Access Point Network (APN) service. Using LTE/4G (or potentially even 5G connectivity as it is brought to market), this service allows for secure connectivity through our mobility infrastructure, to connect back into the County network's AVPN edge at the County Operations Center and AT&T POP. While this solution eliminates the "last mile" single point of failure, early deployments using the LTE network will need testing to fully assess the impact of potential latency issues. As we look further down the industry roadmap, advancements promised in 5G connectivity have the potential of providing a high speed, low latency service that could meet enterprise requirements.

Through a collaborative evaluation of these options, HPES, in conjunction with the County, will develop a roadmap to migrate all T1 based technology to connectivity options which are in line with our geo-redundant core infrastructure. Figure 179 illustrates this concept.

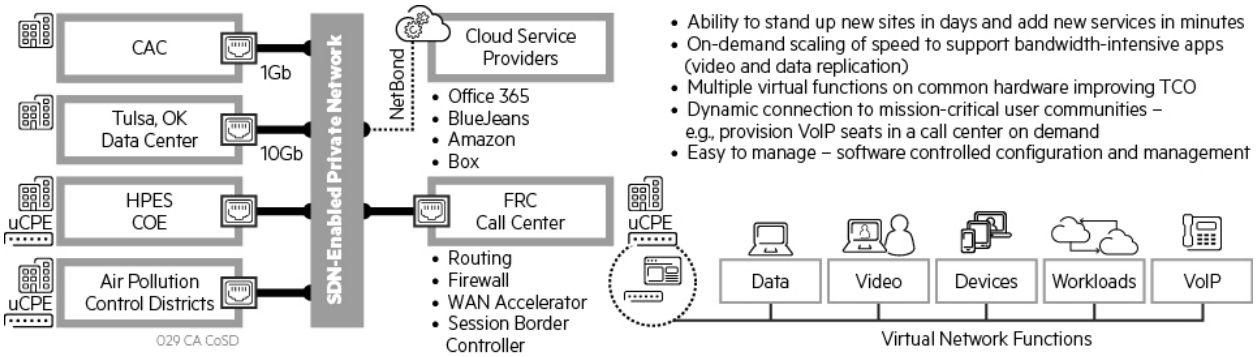
Figure 179. Commercial Connectivity Service – Enterprise Secure Connectivity using AT&T's LTE Mobile Network



Future Evolution of Software-Defined Networking-Based Services

During the life of the contract, AT&T will continually expand and improve its software-defined network (SDN) capabilities, where the local AT&T County network team will evaluate and recommend upgrades as they become viable and align with existing services. Midway through the next contract term, we anticipate key technical advances that could fundamentally affect the topology of the County network and the capital investment strategy. Building on the SDN foundation, new universal devices (Universal Customer Premises Equipment, or uCPE) could potentially represent a paradigm shift in how networks are provisioned and managed. Shifting capital cost to the provider, the County can take advantage of Network Function Virtualization, which provides services such as integrated LTE broadband backup, firewall, WAN optimization, and voice gateway functionality all on the same carrier managed device. Using our collaborative approach, we will conduct production pilots, evaluate feasibility, determine business value, and make recommendations through the established Enterprise Architecture review process. Figure 180 illustrates the AT&T SDN enabled enterprise of the future.

Figure 180. AT&T SDN-Enabled Enterprise of the Future



As the needs of the County continue to evolve, we will continue to collaborate with business unit and CTO staff and our cross-framework partners to understand the challenges and develop best-in-class solutions. We believe that transformation is an iterative process, requiring strategic planning and vision coupled with practical approaches that ultimately make certain that functionality is provided to the customer in the most expedient way possible. Technologies identified in this solution are just the beginning of a contract lifecycle of change, but will provide a foundation for growth as we move forward as a trusted advisor to the County.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The local, dedicated AT&T team—fully embedded in the solution lifecycle—provides all design, implementation, support, and monitoring of transformation activities. Technical personnel assigned to the County of San Diego and dedicated to the program are located at our Trade Street facility to maintain a fairly central base from which to service the County. All solutions leverage the AT&T Internet Data Center (IDC) in San Diego County as well as the County's Operations Center to hold the core hardware components and facilitate circuit terminations. Working from the local Trade Street facility, our SMEs will monitor, support, and maintain the remote services.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

The local, dedicated AT&T team views transformation as an ongoing activity. By constantly monitoring what is currently available technology as well as keeping abreast emerging technology, we are able to deliver concepts and ideas for consideration by the CTO. We have already begun the task of installing ASE w/NOD at all new County sites; this task was preceded by the installation of two new host circuits, one each at the point of presence (POP) and County Operations Center (COC). We will leverage this existing infrastructure as we begin migration to ASE from the existing OPT-E-MAN connected county sites, with our project management staff coordinating the implementation(s). Work is also currently underway to consolidate the core GigaMAN backbone sites, with high-level architecture design already underway. The expectation is that the first two sites will be transitioned by approximately the end of the year.

Discussions with the County have already begun and are continuing related to cloud providers and the benefits that NetBond can provide. AT&T remains dedicated, so when and if the County decides this service is necessary—based on migration of various components to cloud providers and infrastructure—the local, dedicated AT&T team will bring in any resources needed to facilitate the entire process. This process will span final design and associated documentation, ordering of infrastructure components like circuits, and coordination with AT&T core services as well as cloud providers to provide a seamless transition. The local, dedicated AT&T team will continue to leverage all resources available within our

local organizations (Engineering, Project Management, and Architecture) to provide all aspects of transition and transformation activities.

- Automated Tools – Automated systems and tools involved in proposed solution

The local, dedicated AT&T team uses a myriad of tools and automated systems to perform implementations and support operations and performance. These tools include Cisco Prime Infrastructure, the CA Spectrum suite, SNTC (Smart Net Total Care), Riverbed Cascade, and Panorama. Cisco Prime Infrastructure is used to centrally manage configuration as well as gather data related to changes, performance, inventory, and licensing. The CA Spectrum suite—which includes Spectrum and E-health—is used to monitor availability, performance, and inventory management; it also provides trending and analysis for traffic utilization. SNTC is a Cisco product used to manage support services as well as automate the process of gathering data for direct vendor support in the event of a problem. Riverbed Cascade is a deep packet analysis tool that uses NetFlow data, which is gathered passively and , directed to it in an automated manner as well as active packet capture and analysis. Finally, Panorama is a Palo Alto Networks product that provides a central repository for logging, inventory of the Palo Alto components, licensing management, software image management, and analysis capability for the County security infrastructure.

- Qualifications and Experience – Background and experience in comparable environments

The AT&T team dedicated to the County program consists of network and network security engineers as well as project management and support staff with decades of combined experience in supporting these specific solutions along with 12 years of direct support to the County. The team's knowledge of both the solution and the County maximizes the County's return on investment while minimizing transition risk.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (optional) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

Initiative: Voice Services Transformation (Exhibit KK, Section 3.5)

- Key Considerations and Potential Alternative Approaches

Early in the existing IT Outsourcing contract, as part of the committed transformation of the voice environment, the network team executed a flattening and consolidation of the Avaya infrastructure. As a result of this migration, the core of the voice network was VoIP-enabled across the County WAN. Over the 5-year data network switching refresh, executed from 2007 through 2011, all LAN switching infrastructure was upgraded to Power over Ethernet (PoE)-capable devices. In 2010, the voice network team proposed a complete VoIP solution as a new site standard, extending the technology to either endpoint or telephone set. Since then, our team has deployed more than 6,000 VoIP telephone sets to nearly 20 county facilities.

Over the life of the current agreement, the County's voice strategy has been continually evaluated and adjusted, with a focus on enhanced real-time communication capabilities that eventually became defined by the industry as a convergence of voice, presence, video, and conferencing capabilities into a Unified Communications (UC) solution. Our team has focused on enabling features and functionality across the enterprise, which allowed early adopters to take advantage of these capabilities, recognizing that the foundation of our service is the basic functionality of the telephone used by more than 18,000 end users

on a daily basis. Some of these deployed capabilities include speech to text (voicemail to email), IP soft phone (for daily users as well as contact center agents), extension to cellular and Session Initiation Protocol (SIP) integration.

Maintaining a Voice Services and UC strategy in a dynamic, industry-influenced environment has created challenges that the network team has continually evaluated, adjusting roadmaps accordingly. The long-term objective has been, and continues to be, the ability to provide a single UC client, capable of integrating with or even potentially controlling voice services functionality while providing pervasive and integrated real-time communication capabilities that increase business productivity. The pursuit of this objective requires careful consideration of industry advancements, business requirements, technology adoption rates, user experience, disruption potential, solution integration requirements, and investment timing.

With this background, the AT&T team has defined a transformative and achievable Voice and UC strategy that brings valuable functionality and productivity to end users in a cost-effective manner, while allowing continued strategic planning and evaluation of new industry solutions as they mature. Our transformation approach will focus on eliminating legacy technology, bringing the enterprise to VoIP and removing aging infrastructure. This first step is an important one, as it will standardize the end-user voice experience, enabling the AT&T team to focus on providing an integrated UC capability. By integrating the Avaya enterprise voice infrastructure with the Microsoft Lync (Skype for Business) desktop client, HPES will unlock functionality that will allow the County to take full advantage of new features including telephone presence and click-to-call functionality (through the desktop, extended to the enterprise phone set or even to a mobile device) while presenting the voice call using the enterprise designated phone number (Direct Inward Dialing–DID). Our team believes that these additional capabilities, combined with a fully supported Lync client, will enable a new wave of UC feature adoption as users begin to take advantage of these extensive real-time communications capabilities.

Successful transformation of any kind requires the ability to identify opportunities for change and measure the value of the result against the cost of implementation—be it financial or in disruption to the norm—while also supporting foundational requirements such as allowing all County telephone numbers to stay the same. Over the lifecycle of the proposed solution, AT&T will continually evaluate these opportunities, establishing milestones for key decision points that could bring forward new approaches, consolidate functionality, or represent cost savings to the County. These options may include a natural migration path of localized premises-based services to a cloud-based, fully hosted off-premises architecture. Through ongoing roadmap planning and collaboration with the County Technology Office, we will advance the Voice Services and UC transformation strategy throughout the contract lifecycle.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

The solutions highlighted in this section include transformation initiatives planned for implementation early in the term as well evolutionary technologies that may arise later in the contract life cycle. In the near term, all defined solutions represent planned implementations that are inherent to the services described in Section 4.3 of the RFP and are priced in Exhibit 16.1-1 accordingly. Relative to statements focused on technology not yet available for deployment, AT&T will roadmap and evaluate the feasibility of these solutions during the contract life cycle. If identified as a viable replacement to existing services, AT&T will make recommendations for upgrades in line with refresh obligations or as otherwise agreed with the County.

AT&T's approach to transforming voice services focuses on enabling new features and capabilities used by both the end users and County constituents built on a foundation that is redundant, resilient, and highly available. The ultimate goal in developing the next architecture for voice services is to harden the core

and edge locations and to offer robust and feature-rich UC for each and every user of enterprise voice services.

Core Network Transformation

Transformation activities at the Avaya Voice Core will migrate from any remaining traditional PBX architecture and provide an infrastructure reduction resulting in lower power consumption and reduced trouble tickets while minimizing disruption to users. This approach provides migration from the existing G650 Port carriers or other gateways, and upgrades them to G450 or G430 gateways. This transition will eliminate legacy IP Server Interface (IPSI) boards, mitigating risk by replacing end-of-life equipment and reducing the physical footprint in the data centers. This transition will take place at the Point of Presence POP as well as the County Operations Center (COC). In addition, the "TN" modules will be replaced with Media Modules in the G450s or G430s, and the digital signal processor (DSP) resources will be replaced with local media resources at the gateway as well as in the Avaya media servers.

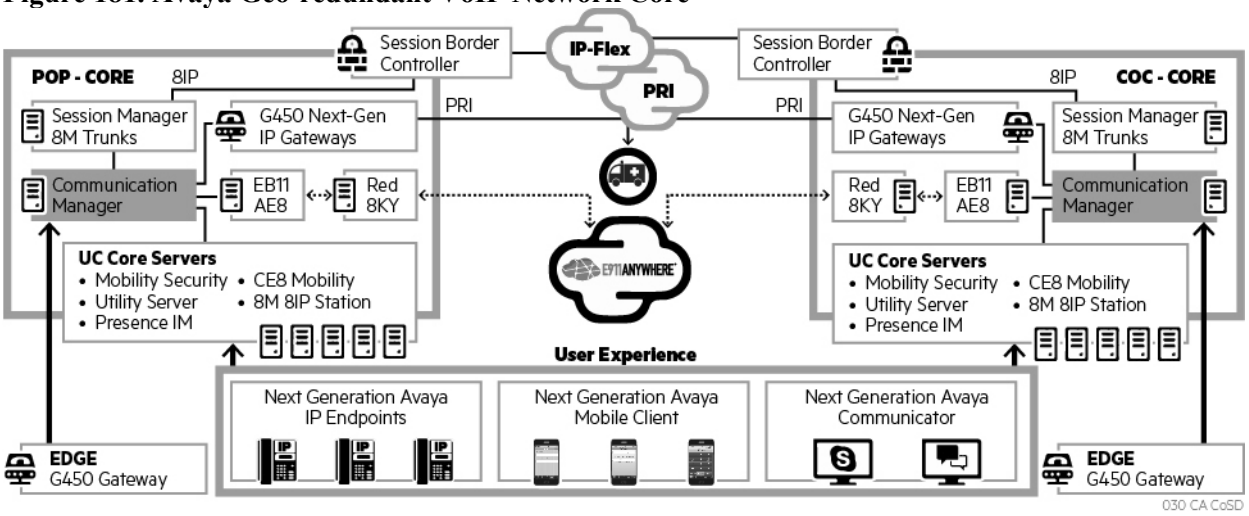
This highly available architecture will provide seamless failover between the COC and POP, with no single point of failure of the Core VoIP gateways. The proposed architecture not only will provide centralized management between the two "Core" locations—POP and COC—but will also provide access to the remote locations, or locally survivable processor (LSP) sites.

Additional implementations will take place at the Core that will serve as the foundation for offering new and enhanced UC capabilities for end users, such as external mobile SIP endpoints on County- managed devices. This will be made possible by the Avaya Client Enablement Server as well as the Avaya Presence service for telephony presence on a mobile device.

Geo-redundant Voicemail

Our proposed solution includes the advancement and transformation of enterprise voicemail services, which replace the current, single-site-based voice messaging platform located at the AT&T POP, with a fault-tolerant, geo-redundant voice messaging platform located at the AT&T POP and COC. The new platform provides the ability for a standardized voicemail experience across all of the County's Avaya enterprise voice locations. This geo-redundant design incorporates live replication of the voicemail database, messages, and greetings between the AVST Call Servers at the AT&T POP and County Operations Center using AVST's never fail technology. Figure 181 illustrates the Avaya Geo-redundant VoIP Network Core. This solution is expected to be in place as the next agreement is signed. Using a roadmap strategy, AT&T Centrex users will be migrated over time to this platform, as specified below in the paragraph highlighting AT&T's Centrex migration roadmap.

Figure 181. Avaya Geo-redundant VoIP Network Core



The new platform provides the ability for a standardized voicemail experience across all of the County's Avaya enterprise voice locations.

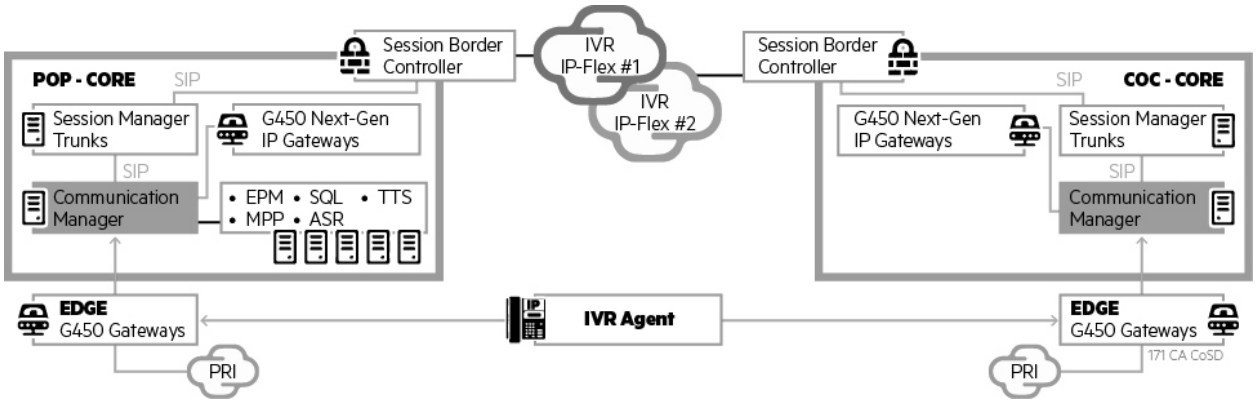
Interactive Voice Response (IVR) Transformation

Lastly, AT&T's transformation plan for Voice Services extends to Core adjunct services, such as its Interactive Voice Response (IVR) solution. The County's IVR infrastructure is built around the Avaya experience portal, which is a high availability contact center solution located at the AT&T POP. This platform provides access for external constituent service to County departments (such as Animal Services, Land Use Environmental Group, and various departments within the Health Human Services Agency) using features such as IVR, self-service, touch-tone, and speech recognition services. This scalable, high availability infrastructure provides many options for programming and agent integration, allowing customization for any type of constituent-facing contact center service.

The platform will undergo near term changes to external telephony connectivity as AT&T initiates plans to implement dedicated, fault tolerant inbound and outbound IP flex SIP trunks for the County's IVR infrastructure at the AT&T POP and County Operation Center. This change will prevent the Core IVR solution from impacting enterprise voice traffic, allowing business units to conduct high volume contact center activities such as outbound dialing campaigns. This new capability will provide a more standardized RU that business units can use to leverage the platform in meeting their business needs.

Over the term of the contract, AT&T will focus on roadmap initiatives and develop proposals to increase redundancy and resiliency of Core IVR applications as well as provide additional feature benefits such as automated agent call back and web chat.

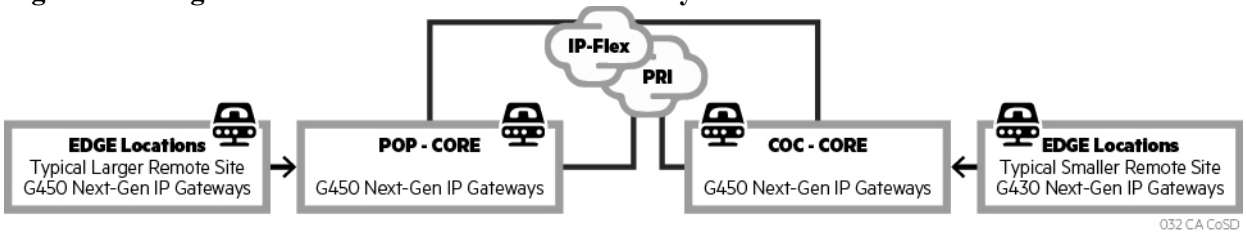
Figure 182. Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.



Edge Network Transformation

At the remote Edge, AT&T will replace all legacy cabinets and gateways (G650, MCC, SCC, CMC, and G700 series) with the latest generation of G450 or G430 gateways, providing LSP for resiliency. In the County, 81 sites have been identified as needing remote edge transformation to accommodate the implementation of VoIP phones. These 81 locations currently have digital telephones served from legacy cabinets and gateways. The Avaya G450 Media Gateway is a multi-purpose media gateway. Figure 183 illustrates Edge or Remote Site Network Connectivity. It works in conjunction with Avaya Communication Manager IP telephony software running on Avaya S8XXX Servers to help deliver intelligent communications to enterprises of all sizes. The G450 combines telephone exchange and data networking by providing public switched telephone network (PSTN) toll bypass and routing data and VoIP traffic over the WAN. The G450 features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity. The G450 provides full support for Avaya IP and digital telephones as well as analog devices such as modems, fax machines, and telephones. Telephone services on a G450 are controlled by an Avaya S8XXX Server operating either as an External Call Controller (ECC) or as an Internal Call Controller (ICC). The G450 supports the Avaya S8300 Server as an ICC or, when the S8300 is installed in another media gateway, as an ECC. An ICC will be installed and used as a LSP. This is designed to take over call control in the event the ECC fails or the WAN link between the branch office and main location breaks. The LSP provides full-featured telephone service survivability for the branch office. The G450 itself also features Standard Local Survivability (SLS), which provides basic telephone services in the event that the connection with the primary ECC is lost.

Figure 183. Edge or Remote Site Network Connectivity



Centrex Migration

As detailed in Volume 2 – 2.08 Section 5.7 of Voice Services, the majority of voice services for the County are provided by the Avaya enterprise voice network. A small subset of the County's office sites do have voice services delivered by AT&T's Centrex business telephone service. Centrex service is typically deployed to smaller County sites that contain 1-20 users. At present, there are roughly 117 sites

with Centrex voice services. While the AT&T Centrex business telephone services provide stable telephony and voicemail services, these locations are separated from the remainder of the County's user population and are not able to take advantage of the full UC capabilities offered to Avaya enterprise users. With this in mind, the need to transform the features and capabilities for current Centrex voice services locations and to enable the users with the ability to use Avaya enterprise voice feature is a business priority. AT&T has developed a transformation approach to migrate a majority of these users' stations to a VoIP solution, while maintaining a roadmap for remote and intentionally off-net services to be executed during the term of the agreement.

The migration of Centrex users will begin with the deployment of stand-alone IP-based telephones at sites with existing data network functionality. This solution will provide services for VoIP telephone sets that is centrally managed by the Avaya geo-redundant voice cores at the AT&T POP and County Operations Center. While these sites will not have local survivable gateways, they will take advantage of the data network for their connectivity to the enterprise voice infrastructure. Of the roughly 117 Centrex sites across the County, 80 of these locations would be eligible for this service. Through this migration, over 65% of the Centrex remote sites and more than 272 individual stations will be converted to the Avaya enterprise standard. These sites/users will be provided new centralized voicemail and UC functionality as well as a new telephone set that leverages the County's investment in the data network for connectivity.

A greater challenge in the elimination of the legacy Centrex solution is associated with locations that do not have data network access. These locations are typically very small and remote locations that only require simple telephone service for communication. The migration of these services will be the topic of transformative roadmap planning during the term of the new contract. Currently, AT&T is developing a Centrex replacement technology that is expected to provide transport and service options that will be evaluated for transformation. Some additional possibilities include the use of the mobility network for connectivity to the enterprise infrastructure, using an emerging technology called voice over LTE (Long Term Evolution).

Additionally, there are some remaining Centrex stations that have been placed throughout the County in locations with data network services where off-net phones are provided as a business requirement, such as elevator phones and emergency lines (red phones). As the Centrex replacement solutions mature, these solutions will also be evaluated for migration to a similar, off-network service so as to maintain the redundancy required for the specific use case.

VoIP Telephone Standard

The End-User experience is the single greatest change that will affect the County users in the proposed voice transformation. While the voice network is continually upgraded at the core, many telephone sets across the County have remained unchanged in over 15 years. By moving to new VoIP telephone sets, the County users will enjoy the benefits of a new device, along with improved reliability and performance.

There is significant value in resiliency that IP telephones offer over legacy TDM telephones. TDM devices require a dedicated port with a dedicated wire to connect to a local gateway. There are many points of potential failure, including the wire, gateway card, gateway power supply, gateway processor, and so forth. An IP telephone connects universally to any network port to facilitate registration to one of several points of call processing. An IP telephone will primarily be registered to the Session Manager Registrar at the core; there is a Session Manager Registrar at both core sites for high availability. In the event an edge location becomes fragmented from the WAN, the IP telephone will register locally to the G450 gateway with a local survivable processor (LSP).

Avaya/Skype for Business Integration

Another important pairing with a VoIP deployment is the implementation of E911 services. E911 allows for a continually managed registry of location data for each workstation so first responders have necessary information to effectively respond to an emergency call (see Exhibit KK – Section 3.7. E911).

Another key end-user benefit associated with the Voice Transformation initiative is the integration of the Avaya enterprise voice system with Microsoft Lync (Skype for Business client). Using available licensing and open Application Programming Interfaces (API's), **Avaya Communicator** extends Avaya Aura real-time collaboration capabilities to Microsoft Lync 2010, 2013, or Skype for Business 2015, 2016 clients to provide users with a unified, consistent collaboration experience from their preferred applications and devices. The Avaya Communicator for Microsoft Lync service adds functionality to Microsoft Lync clients using only the Lync/Skype for Business standard client access license (CAL). Features include telephony presence aggregated with Lync's machine and calendar presence through Lync/Skype for Business client API and Lync/Skype for Business IM and desktop sharing, click-to-call control of PBX desk phones, voice and video, enterprise dial-plan support, toast pop-ups enabling incoming calls to be answered, and Reply with IM as well as a conversation window pop-up to access Avaya mid-call features and the ability through the Share My Bridge feature to launch a conference call and or collaboration session from within the client.

Avaya Collaboration Services

Avaya Collaboration Services interworks on the user PC with Communicator for Lync to provide UC services originated from Microsoft Office Suite, Outlook, SharePoint, and Internet Explorer as well as Mozilla Firefox and Google Chrome browsers.

When in Outlook or SharePoint, hovering over a user's name or presence indicator presents their contact details. The user now has the opportunity to IM, email, make a voice or video call, or schedule a meeting with this user. The user's presence is also displayed.

In addition, Collaboration Services will detect a number embedded in an email or a Word, Excel, PowerPoint, or SharePoint document and allow calls to be made to this number through Communicator for Lync. As with a call originated through the Lync/ Skype for Business user interface, a conversation window will be presented to provide the user with call control options for the duration of the call.

Collaboration Services automates the process of Join or Host a conference call. With this feature, the user can launch a conference call and/or a web collaboration session. The Collaboration Services will determine whether the user is the Host or a Participant to this call and uses the appropriate access passwords to access this call.

Collaboration Services, when used with Internet Explorer, Mozilla Firefox, and Google Chrome browsers, will recognize number patterns on web pages, and through the use of an intelligent algorithm applies enterprise, national, and/or international dialing rules to highlight these as phone numbers. These phone numbers can be dialed from a web site using the Avaya Communicator for Lync.

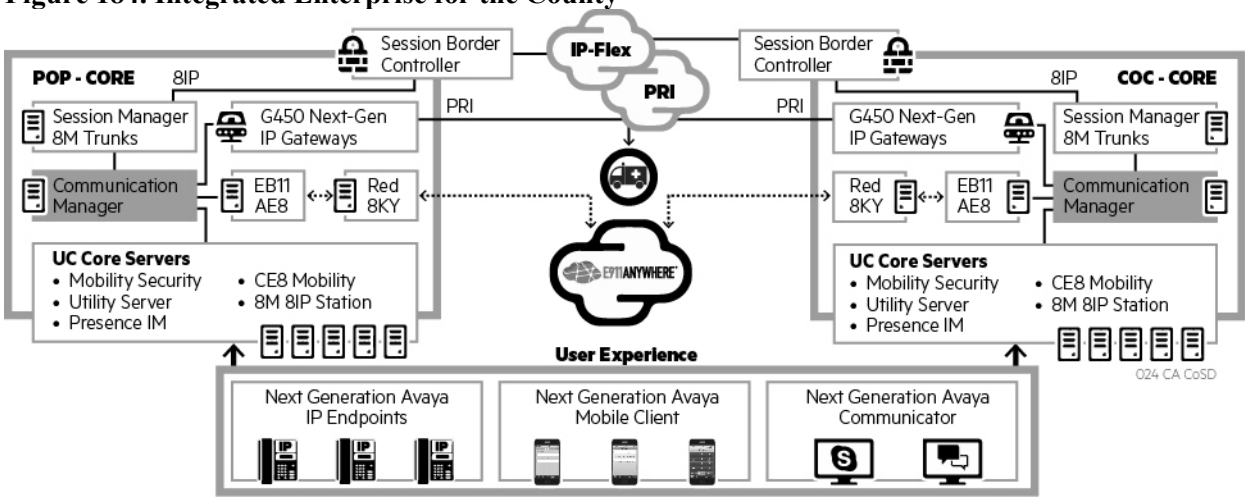
If a phone number is on an enterprise web page, Collaboration Services will take this number, access Active Directory, and pull down additional information for this user. This information is displayed on a contact card. The contact card is also populated with icons that enable the user to send an IM and see the presence of this contact, make a voice or video call to the contact, and schedule a meeting.

Integrated Enterprise Mobility

A final end-user benefit of the Voice Transformation initiative is integration of the user's voice and UC capabilities with their mobile device. Integrated Enterprise Mobility brings seamless interoperability with

the desktop and desk phone. Figure 184 illustrate components of the County Integrated Enterprise experience.

Figure 184. Integrated Enterprise for the County



Integrated Enterprise Mobility brings seamless interoperability with the desktop and desk phone.

Features that span the desktop and desk phone are extended to the mobile user and are transparent in functionality. Examples include the following:

- Start a call from your desk (either desktop client or desk phone) and, if you choose to become mobile, simply select a button on the mobile app to move the call from the original location to the mobile device.
- Call processing from a mobile device extends a robust feature set (Hold, Transfer, Conference, Speaker, Mute, etc.) to the user so that transitioning from desktop or desk phone is seamless. The user experience is the same.
- The UC features of Avaya Communicator include visual voice mail to filter and sort voice messages. Use the visual voice mail feature to respond to important messages quickly. Communication History logs help you trace the history of your enterprise calls and voice messages. Use Avaya Communicator to increase the productivity of your enterprise with tools that enhance collaboration, improve responsiveness, and lower costs for IT and end-user support.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The local, dedicated team provides all the design, implementation, support, and monitoring of transformation activities and is fully embedded in the solution life cycle. Technical personnel assigned to the County are dedicated to the program and located at our Trade Street location, maintaining a central location from which to service the County. Additional leveraged resources may be engaged to support transformation and will operate under the direction of the local team.

All solutions use the AT&T POP as well as the County's Operations Center to hold the core hardware components and facilitate circuit terminations. All County facilities with voice network connectivity will house infrastructure and telephone sets necessary to provide service.

Methodology & Key Processes – Key methodologies and processes in proposed solution

The dedicated LCM team is embedded in the full life cycle of every enterprise voice and UC solution—from the initial gathering of requirements, through the design and implementation phases, to managing

and monitoring, and even decommissioning when requested. Through customer meetings and service reviews, the team creates the proper solution that is chosen and sized appropriately.

We will use standard Project Management methodologies in the scoping and execution of any new installation. AT&T architects and engineers will also use approved processes in their design and equipment placement activities. Enterprise voice and UC options are continually evaluated based on County business requirements in addition to current and emerging technologies.

Our technical enterprise architecture team evaluates new products and standards to make recommendations to the CTO. When a recommendation is approved, our team moves forward with implementation recommendations including refresh of existing equipment and rollout schedules. For equipment issues, our Service Desk and engineering team work to identify and remediate the problem.

- Automated Tools – Automated systems and tools involved in proposed solution

To support quality voice service within the support levels defined by the new agreement, our subject matter experts (SMEs) use numerous automated tools. These tools enable us to continuously monitor the overall health and performance of voice appliances, provide tools to assist in rapid restoration through fault isolation, and perform traffic analysis, as discussed below.

HPES delivers complete manufacturer system maintenance coverage on all County Core Voice Services assets. The Avaya maintenance services include Avaya Expert Systems and Secure Access Link. Avaya Expert Systems provides the County Core Voice Services a maintenance database of more than 30,000 Artificial Intelligence Algorithms (AIAs) with scripted automation that is able to automatically correct many known system and software-related issues. Avaya Secure Access Link (SAL) is a centralized consolidation point for all Avaya Core systems for health and alarming monitoring, secure remote access using secure outbound-only HTTPS standards, and an integration point for Avaya Expert Systems. Together, these tools provide the County's Avaya Core Voice Services complete health monitoring and rapid issue resolution. Avaya Expert Systems and Secure Access Link are online and engaged 24/7 to diagnose and attempt to resolve known system alarms, clear many service-affecting issues, and escalate to engineering resources for prompt attention when necessary to allow service restoration or outage avoidance to County users.

Our Voice Services team uses Nectar's Unified Communication Management Platform (UCMP) and leverages its complete suite of innovative features to provide the County enhanced integrated UC network services. Nectar provides multi-vendor management services including application dependency tree visual alerting and vendor knowledge modules, which assist our SMEs to proactively pinpoint and resolve cross-platform integrations issues to quickly restore services to County users. The UCMP also includes real-time network quality-of-service reporting using RTP (Real-time Transport Protocol) Control Protocol (RTCP) integration and can provide our team with the capability to create simulated traffic injection between designated network segments for analysis. This enable SMEs to monitor and report on all VoIP-related traffic transmissions. The quality-of-service reporting tool provides per-hop statistics, and in many cases assists in quickly identifying improper packet handling hop points, driving efficient resolution of network quality-of-service issues. The Nectar platform includes statistical resource utilization data gathering and storage that enables trending analysis and capacity planning so County users are not impacted by growing resource needs. Finally, all these capabilities are wrapped into an intuitive and customizable dashboard for use with visual and electronic alerting from sophisticated threshold configurations that drive the ability to acknowledge, respond to, and correct issues proactively in many cases before County users are aware of or report an issue.

E911 Manager will automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T MPLS network to track and update VoIP, digital, and analog phone moves, adds, and changes.

E911 Anywhere is a cloud-based 911 call routing service that can connect a 911 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada.

- Qualifications and Experience – Background and experience in comparable environments

Our team's support specialists participate regularly in internal and manufacturer-led training programs. We hold certifications specifically related to Voice Transformation and UC systems and have been recognized by technology leaders for our support expertise. Our certifications include the following:

- Avaya Certified Expert–IP Telephony
- Avaya Certified Implementation Specialist–Unified Communications
- Avaya Certified Implementation Specialist–Contact Center
- Avaya Certified Solution Specialist
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Professional (CCNP)
- Microsoft Certified Solutions Expert–Lync Master

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

Initiative: Storage Architecture (Exhibit KK, Section 3.6)

As the County relies more heavily on electronic transactions to streamline services to citizens, data volumes will continue to grow. Currently, the County generates and currently manages nearly 100 TB of unstructured data, and, as the volume continues to grow, storage costs grow as well. Cost effectively managing the growth requires better data management policy and procedures and better targeting data to cheaper storage aligned with County's need to access the data as well as exploring newer storage technology.

The solution to this transformation project requires a blend of process and technology, hardware and software. Section 2.9 (Schedule 4.3, Section 6.12) of this proposal describes a tiered storage approach that addresses the County's immediate needs. The Solution Summary section below describes how we will meet the County's longer-term storage needs. We also recognize that the County's needs and storage options will evolve, and, as they do, HPES will continue to identify technologies that provide the County the most value.

In Exhibit KK, Section 3.6, the County identified four specific initiatives that are tied to Storage Architecture, which we address individually in the following sections. These initiatives are as follows:

- Architect storage to embrace tiers of well-defined storage
- Classify County data and assign it to the appropriate tier
- Develop archival solutions for Portfolio applications
- Develop Hyper Converged Integrated Systems

- Key Considerations and Potential Alternative Approaches

Architect Storage to Embrace Tiers of Well-Defined Storage: The solution being implemented by HPES during the data center consolidation architects the design to embrace tiers of well-defined storage. The key considerations that went into the storage solution include cost and the ability to meet the

County's requirement to keep the storage infrastructure current by refreshing storage components every 5 years. We also considered the storage growth requirements and developed a solution with 20% year-over-year growth projected for the first 5 years.

In addition to our proposed solution, which builds on the storage that will be in place for the County on completion of the transition activities, HPES considered two alternatives:

Storage Tiering Alternative: HPES considered providing a 3PAR 20000 with 15,000 RPM drives and/or SSD as Tier 1, 10,000 RPM drives as Tier 2, and 7,200 RPM drives as the archive tier. This would provide a clearer delineation of the tiers from a performance perspective but would have resulted in a higher total storage cost than our actual solution. We will continually monitor the performance of the storage environment and offer

Shared Storage Alternative: The second alternative is to provide storage as a leveraged service. This approach is similar to cloud storage in that the storage infrastructure would be shared with other non-County of San Diego clients, but the storage volumes would be dedicated to the County of San Diego. There would be no co-mingling of data on storage volumes, but the underlying storage hardware would be shared. All storage volumes would be securely wiped after they are no longer needed by the County, to prevent any chance of the County's data being exposed to non-County of San Diego customers on the leveraged storage infrastructure. This solution provides a lower cost per GB of storage. Using leveraged storage, we could also provide the required tiers of storage using either the recommended solution or the Storing Tiering Alternative. However, with this leveraged approach, the County would not be able to specify the hardware refresh to meet their desired schedule, so we rejected this solution.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Solution Summary: Upon completion of the data center consolidation, the storage architecture will comprise a dedicated storage area network (SAN) with a 3PAR 20000 storage array in Tulsa providing tier 1, 2, and archive storage to all data center servers, consolidated in Tulsa. End-user data storage will be provided directly from the new network-attached storage (NAS)-capable 3PAR. Otherwise, end-user data storage will be the same. All 3PAR data will be backed up locally using HPE Data Protector with a StoreOnce Virtual Tape Library (VTL) as the backup target. All backup data and disaster recovery (DR)-required 3PAR data will be replicated to the DR site in Colorado Springs. The data center solution will include immutable storage, which will also be replicated to the DR site. For the San Diego sites, backup data will be replicated to the DR site instead of being copied to tapes, for remote offsite storage. Finally, the immutable storage refresh and reconfiguration will be a newer version of the same immutable storage.

The HPES storage architecture following transition includes updated storage equipment, which will be refreshed on a 5-year cycle. The storage array technology is flexible and efficient, designed to keep pace with the County's requirements as they evolve. Tiers 1 and 2 have been redefined to reduce cost without sacrificing performance. The backup solution will consolidate all of the County's backup needs into one capacity-driven solution that eliminates physical tapes from the environment. The location of the immutable storage solution will change with the Data Center Consolidation, and the hardware will be refreshed.

HPES will continually evaluate the various storage tiers used by the County as their storage requirements evolve, with an eye toward providing the right storage solution for each tier. However, the storage solution that will be in place following Transition provides ample opportunity for growth in terms of storage and performance, as described and illustrated in Section 2.9 in response to Schedule 4.3, Section 6.12. Tier 1, Tier 2, and achieve tier storage service is based on 3PAR 20000 storage devices—the latest innovation in 3PAR enterprise storage from HPE.

We will continually evaluate the County's storage archiving needs and consider a cloud-based archive storage solution if/when cloud-based archiving meets the County's approval.

Rationale: The solution we provide meets the County's post transition requirements and will allow the County to transform its storage architecture over time, as needed. The 3PAR is capable of supporting 15 PB of usable storage capacity. It will support a range of disk drive technologies from 7,200 RMP, 10,000 RPM, and 15,000 RPM Serial Attached SCSI (SAS) drives and solid state disk drives (SSD). The 3PAR supports storage migration without interruption via 3PAR-enabled storage peer motion (SPM). The 3PAR supports the following:

- Thin provisioning (TP), which is a method of optimizing the efficiency with which the available space is used in SANs. TP operates by allocating disk storage space in a flexible manner among multiple users, based on the minimum space required by each user at any given time.
- Auto tiering is a real-time intelligent mechanism that continuously positions data on the appropriate class of storage based on how frequently the data is accessed. This improves application performance.
- Compression, which reduces the number of bits needed to store or transmit data.
- Data deduplication, which reduces storage needs by eliminating redundant data. Only one unique instance of the data is actually retained on storage media.
- Federal Information Processing Standard (FIPS) 140-2—data at rest encryption to protect against loss or theft.
- Industry standard redundant array of independent disks (RAID) configurations to meet disk fault tolerance requirements and optimize performance.
- Remote and local replication for future refresh migrations on live data (meaning no down time required).
- Quality of Service to make certain bandwidth is available when needed.

The immutable storage solution has the capacity to support future growth in data storage requirements. The County's Document Processing Center (DPC) storage, which also uses 3PAR, will allow the DPC storage to evolve as needed. The direct attached storage will remain the same, and HPES will continually evaluate services that use direct attached storage and work with the County to determine when/if those services can be migrated to SAN and/or cloud storage.

Timing: HPES performs weekly reviews to assess capacity usage and determine whether changes are needed, taking into account any anticipated changes from the County.

Risk Considerations: This approach poses minimal risk based on continued use of the same platform. All capabilities are currently available, and the County can take advantage of this on a schedule that meets its needs.

Key Dependencies and Milestones: None.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

The HPES Storage Administration team will perform the assessments on an ongoing basis, as described above.

Storage hardware will be located in the Tulsa data center and at the San Diego sites, which include the DPCs at Lemon Grove and Viewridge. The storage will be replicated to the DR site in Colorado Springs.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

At the 5-year refresh cycle, we will continue to use replication extensively. Our storage administration staff is well versed in array-based replication capabilities and will be able to extend replication to include the new hardware with little to no disruption to the County's compute services.

- Automated Tools – Automated systems and tools involved in proposed solution

Enterprise storage (3PAR) has native replication capabilities built in and enabled by the storage array software. The primary tool used to accomplish the storage transformation will be SPM. This type of replication is automated and keeps storage in sync on both copies of the data.

- Qualifications and Experience – Background and experience in comparable environments

HPES has proven experience providing these types of services to a variety of clients with environments similar to that of the County, as described below.

County of San Diego: We have demonstrated our ability to meet these requirements under our current contract with the County. Our storage administration staff is using the tools needed to accomplish the transformation to a tiered storage architecture on a daily basis and will continue to use the tools as part of ongoing operations and maintenance (O&M).

Department of Navy (DON), Next Generation Enterprise Network (NGEN) contract, which includes support for the Navy Marine Corps Intranet (NMCI): From 2005 until early 2014, our team managed and monitored a diverse SAN environment that consisted of two different vendors' SANs. In mid-2014, the team designed, engineered, and implemented a one-platform SAN environment to standardize NMCI on the more flexible, easy-to-use and support NetApp SANs. At that time, our team replaced all non-NetApp storage to achieve a single-vendor SAN environment with a single set of tools, reports, and storage allocation techniques. This single-SAN approach has enabled us to capitalize on native capabilities to provide site-to-site resiliency and reduce backup overhead through a storage hub and tapeless backup. Our single-SAN design is reducing complexity and total operating cost while increasing operating efficiencies and effectiveness.

HPES has executed a storage architecture redesign that has moved from a standalone storage environment into a clustered virtual storage environment on NetApp Data ONTAP 8.2. This has reduced the managed storage footprint in the server farm by merging disk capacity and controller resources into a single virtual storage fabric while increasing the total capacity to 16 PB. Disk capacity and performance are metrics that can be managed across all nodes in the cluster under a single administrative interface. Compared to the previous version of Data ONTAP, this was managed on a controller-by-controller basis. Clustered Data ONTAP has enabled new efficiencies in the TOC to include labor, tooling, and infrastructure. We are able to maximize resource use by using complementary workload characteristics, dynamically identified to balance utilization. Clustered Data ONTAP facilitates shifting workloads across the nodes without impacting the solutions and users that depend on these services. Figure 185 and Figure 186 summarize the average end-user network storage requirements and minimum storage requirements, respectively.

Figure 185. Average End-User Network Storage Requirements

	Personal File Storage	Primary Mailbox Storage		Command Storage	Records Management	DV End Users Only	Public Folders
VIP	10 GB/User	10 GB/User		2 GB/User	2 GB/User	30 GB/User	1 TB / Claimant
MOC	10 GB/User	6 GB/User		2 GB/User	2 GB/User	30 GB/User	1 TB / Claimant
Business	5 GB/User	2 GB/User		2 GB/User	2 GB/User	30 GB/User	1 TB / Claimant

Figure 186. Minimum Storage Requirements

	Class I	Class II	Class III
	Enterprise Class	Mid-Tier	Economy
Drive Type	15K Revoltions per Minute (RPM) Serial Attached SCSI (SAS) or better	10K RPM SAS or better	7200 RPM SATA or better
Performance IOPS per Array [minimum 25 disk depth per Logical Unit Number (LUN) set]	Greater than or equal to 2100	Greater than or equal to 1500	Greater than or equal to 900
Performance IOPS per Disk	Greater than or equal to 175	Greater than or equal to 125	Greater than or equal to 75
Availability inside the Data Center	99.990%	99.900%	99.000%
Data Types	Virtual machine OS, SQL databases for portal environments with high access, and other high IOPS applications	Mailbox stores, organization file stores, PST, and individual file shares	Archive, deduplication repository, and records management archive
Battery Backup	Yes	Yes	Yes

- Key Considerations and Potential Alternative Approaches

Classify County data and assign it to the appropriate tier: When evaluating solutions to classify County data, we took the following items into consideration:

- The significant volume of the County's unstructured data currently stored in file shares, SharePoint, Exchange, and a range of other repositories; however, not all unstructured data should be treated the same way.
- It is important to be able to classify data based on its importance, sensitivity, and need for access.
- By classifying unstructured data, we can automatically direct it to appropriate data tiers to reduce storage costs while providing the County with the appropriate access requirements.

This initiative, is a primarily technology-driven effort coupled with consulting services to guide configuration of the solution. The alternative approaches are tied to specific implementation models for the various product suites that could be used to deliver this auto-classification.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Currently, a wide range of products is available to support the automatic classification of unstructured data/content. Through the application of policy enforcement, content can be targeted to different tiers of storage. The County has assessed a range of these products and has found several that appear to meet the requirements. We will work with the County to design, configure, and implement the selected product suite.

We would recommend, however, the County implement HPE's ControlPoint software. HPE is recognized by Gartner as a leader in Information Governance and Information Management (IM/IG). ControlPoint provides a robust platform for identifying, analyzing, and managing diverse types of information stored in enterprise repositories. Through continuous monitoring of enterprise repositories, ControlPoint can classify unstructured data based on a range of County identified metadata, including standard classification structure of Public, Sensitive, and Confidential documents, applying policy to facilitate optimal storage strategy.

Rationale: Applying file management tools will help the County to reduce its information footprint by identifying redundant, obsolete, and trivial (ROT) data; this can lead to reduced storage costs.

- Redundant data consists of duplicates such as unauthorized copies of documents, emails, records, or database information residing in file shares, SharePoint sites, mail systems, and databases.
- Obsolete data consists of information that is no longer in use or is out of date. Determining whether data is obsolete can be based on its creation date, last modified date, or access date; then assess this information in conjunction with an appropriate retention policy.
- Trivial data is determined by file type, where the file type has no content value, such as executables, system files, and thumbnails.

Additionally, such a solution can be used to tag and classify unstructured data, and through automatic application of policy, data can be targeted to specific tiers of storage or even deleted if appropriate. Ultimately this will lower the total cost of storage.

Timing: After completion of transition, we recommend approaching unstructured data classification on an enterprise scale. Our approach begins with an assessment and a pilot of a limited set of data/ repositories, while building out the required solution architecture to support the County's entire unstructured data environment. Our solution includes resources to manage the indexing of the remaining data, keep indexing up to date throughout the contract, and cross-train others on the support team.

Risk Considerations: Given the volume of data currently stored by the County, an enterprise-wide implementation can expose significant risk. HPES mitigates the potential risk by starting the project with an early assessment to help define and test the County's data categories. Following the Milestones presented below also mitigates this risk through careful planning and testing prior to enterprise-wide rollout.

Key Dependencies: This solution is dependent on the availability of tiered storage architecture and file management/auto-classification platform, whether ControlPoint or an alternative selected by the County.

Milestones: Key Milestones for the data classification project include the following:

- **Milestone 1 – Develop Data Categories** – Building on the County's existing set of categories such as security classifications—Public, Sensitive, or Confidential—we will use automated tools and common categories to develop a set of categories specific to the County. These categories could include County Groups, Function, and Availability. We will select a set of representative documents from the County's data repositories to use for training and benchmarking. This makes certain that the categories created are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content. Preparation of theses draft categories will not affect documents in production systems.
- **Milestone 2 – Refine and Test** – This step helps to determine the relevance of the categories to enterprise documents. Refining a category is done by adjusting the weighting of a term or the selection threshold, or by adding field text. These activities can be done individually or in combination. A category can be published, making it available for use in automatic policy execution against content managed by the tool suite.
- **Milestone 3 – Auto-Classification** – Once County data is categorized, we apply policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents. Using the desired tool suite, we can automate policy application, governing all aspects of the information lifecycle including deletion prevention, storage management, and ultimately disposition management by applying policies at data creation. Additionally, de-duplicating data across repositories helps to minimize storage costs and reduce discovery times.
- **Milestone 4 – Knowledge Transfer** – Following the pilot effort, further described below as part of our methodology and key processes, and validation of results, HPES subject matter experts (SMEs) will conduct knowledge transfer to the support team for the County to maintain the system and to index all County unstructured data.
- **Milestone 5 – County-wide Rollout**

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES will initially provide a team of SMEs to guide the planning and piloting efforts. This team will work onsite, collaborating with the County's staff and the support team to define requirements and validate the results of the project. This team will also conduct knowledge transfer to facilitate extending the implementation and support County-wide. HPES SMEs will remain available as required to provide reachback support. The infrastructure for the product of choice will be installed in the Tulsa Data Center.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

A data classification project begins by working collaboratively with the County to gain insight and understanding of the legacy data landscape. This helps us to define the benefits of a full legacy data cleanup solution, create a Solution Roadmap illustrating the go-forward plan, and implement the auto-classification solution infrastructure. We then conduct a pilot, where we will sample approximately 1 TB of data currently residing on the County's existing file share environments to determine appropriate classification structure and to demonstrate how data can be targeted automatically to different tiers of storage based on the classification. Additionally, the assessment will showcase where unstructured data exists and how frequently is it being referenced/used so that intelligent decisions can be made regarding data management, archiving, retention, and retirement. Following the pilot, HPES SMEs will perform knowledge transfer to the HPES account team to facilitate indexing of the remaining data and then applying the solution to provide ongoing auto-classification of unstructured data.

- Automated Tools – Automated systems and tools involved in proposed solution

HPES will use ControlPoint software or an alternative platform selected by the County to auto-classify unstructured data.

- Qualifications and Experience – Background and experience in comparable environments

The following example demonstrates HPES qualifications and expertise in classifying data.

Alcatel-Lucent: HP Software and HP Enterprise Services (HPES) developed a complex, groundbreaking solution that featured as-as-service pricing for capturing, retiring, storing, backing up, and analyzing data in legacy applications. The solution employs a range of software products, including ControlPoint and Structured Data Manager. Alcatel-Lucent has committed to retiring 30 applications by Q3 2016, focusing on HR applications. It has scope to retire more than 300 applications in 5 years, each with substantial related data, IT infrastructure, and human resources. The client uses centrally hosted data within HPE's Private Cloud infrastructure under the One HPE IaaS Solution deal won in 2014.

Client Business Needs/Challenge:

- To cut costs and streamline operations, the business wanted to decommission numerous IT systems, creating the need to archive the data from those systems.
- Due to its history as a merged global entity, Alcatel-Lucent had many operating and legacy systems including six different human resources (HR) systems.
- This complexity would increase as the business integrated a third major business, Nokia. In particular, Alcatel-Lucent's chief executive officer (CEO) wanted to retire the enterprise resource planning (ERP) systems.

Client Benefits:

- Lower costs as applications are retired and application data is archived
- Better visibility of its IT environment and data, and ability to search and access a wide range of data from within a single environment
- Improved management of structured and unstructured data reduced into smaller data footprint and lower storage costs

International Criminal Court: The International Criminal Court (ICC) produces and consumes vast amounts of information. Cases could not be tried without witness statements, experts' reports, maps, footage, photographs, and other evidence. Outcomes have to be recorded in judicial documents. These court records need to be stored securely—often for long periods of time—and be easily accessible to those who need and are authorized to use it. Established in 2002 and headquartered in The Hague in the Netherlands, the ICC has a judicial obligation to preserve the vast volumes of information it produces. Governed by the Rome Statute, the ICC is responsible for trying persons accused of the gravest of crimes, including genocide, crimes against humanity, and war crimes.

ICC's records and information management team is responsible for collecting the information from these various specialist areas. They bring it all together, organize it, and present it back to the many people who need to consume and learn from the intelligence it provides. To help the court respond rapidly, the team wanted to map out the diverse categories of information produced by the court. To build the maps, the team first needed to build a clear picture of all the materials produced by court. But with only manual tools available, it took 6 months to build an accurate inventory of the kinds of materials the business was creating. Manual processes were not only slow, they also consumed a lot of valuable manpower.

ICC looked for a tool to help them understand and categorize its information, and they invited HPE to demonstrate ControlPoint's ability to automatically classify data. The international legal institution worked closely with HPE to implement a proof of concept (POC) around HPE ControlPoint that would secure judicial documents, tag operational documents, and dispose of duplicates. As part of the POC, HPE technical specialists were able to demonstrate how HPE ControlPoint could automatically dispose of the outdated and unnecessary legacy content that was consuming storage capacity. The project analyzed around five gigabytes of information stored on ICC's file system, migrating sensitive court records to

their records manager and tagging or disposing of administrative documents according to predefined policies. ICC decided to acquire the HPE solution—a client spokesman commented, "HP ControlPoint helped us to gain visibility into the nature of the records we have. That helped us to speed up the proliferation of our macro retention policy."

Client Business Needs/Challenge:

- Identify and transfer critical court records that needed to be stored safely in the court's record management solution.
- Gain understanding of its information architecture, make certain that sensitive information is stored appropriately, and reduce duplication of records by implementing a system that can identify documents accurately and manage them based on policies.

Client Benefits:

- Frees up resources to focus on higher value activities
- Reduces storage capacity requirements—HPE ControlPoint found approximately 30% of documents to be redundant
- Improved access to data through improved information classification and categorization

- Key Considerations and Potential Alternative Approaches

Develop Archival Solutions for Portfolio Applications: The County has more than 400 applications currently supporting its departments and citizens. These applications rely on different types of data—some unstructured, such as document management and SharePoint oriented data—and some with structured data. It is important to consider and evaluate the full portfolio of applications to determine the appropriateness of data archiving to reduce the data footprint and storage costs. There are two potential alternative approaches:

- **Approach 1:** Conduct an enterprise-wide assessment to determine the applications that should be targeted for data archiving. Based on this assessment, develop an enterprise plan for rolling out the archiving capability.
- **Approach 2:** Start with a pilot effort to validate the cost savings that can be realized by application data archiving. Then conduct an enterprise-wide assessment and develop the roadmap for expanding data archiving.

We recommend Approach 2 because this provides the opportunity for a quick win to both measure the impact of data archiving and to demonstrate its potential to support additional applications across the County. Also, it reduces the near-term investment in hardware and software. Finally, it helps to better define the County's true requirements, which reduces the potential risk of oversizing the enterprise archiving environment.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

HPES sees this initiative focusing primarily on applications that have structured, rather than unstructured, data sources. Recognizing that not all applications have the same potential for data archiving, we will focus on database-to-database archiving as the primary archive model.

A component of the HPES Information Management/Information Governance (IM/IG) Portfolio is the Structured Data Manager (SDM) tool. SDM automates application lifecycle management and structured data optimization by relocating inactive data from expensive production systems and legacy databases,

while preserving data integrity and access. SDM enables retiring outdated applications through an automated process of extracting, validating, and deleting data.

Rationale: This unique solution significantly reduces capital expenses and administrative costs, and helps the County to respond quickly to legal and compliance requests. This enables the County to obtain maximum value from the data.

Timing: This initiative can begin at any time after contract effective date (CED); however, we recommend beginning this initiative after completion of transition. This will make sure that all changes to the data center architecture are complete and will reduce the complexity of implementation.

Risk Considerations: Each application will have to be assessed and evaluated independently to determine the value of archiving data. There is a risk of overestimating the impact of application data archiving, leading to over-solutioning the archiving platform. We address this risk by starting with a pilot effort for a single application that meets a common profile for successful archiving. We will also assist the County to assess other applications and prioritize them for archiving based on the potential for storage or other savings.

Key Dependencies: There are no real dependencies—in fact, the County considered a pilot effort in 2015. However, as stated above, we would recommend delaying the start of this initiative until after completion of the Transition phase of the contract.

Milestones: Key milestones for this initiative include the following:

- Milestone 1 – SDM Requirements and Analysis
- Milestone 2 – Architecture and Solution Design
- Milestone 3 – Foundation Build in Development/Test Environment
- Milestone 4 – Onboarding and Archiving of the Central Reporting System (CRS) Tax Data
- Milestone 6 – Knowledge Transfer and Testing
- Milestone 7 – Foundation Build in Production Environment
- Milestone 8 – Post Production Support and Documentation

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

We will initially provide a team of SMEs to guide the planning and piloting efforts. This team will collaborative onsite with the County's staff and the local support to define requirements and to validate the results of the project. The team will also conduct knowledge transfer to facilitate extending the implementation and support County-wide. HPES SMEs will remain available as required to provide reachback support.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

The County has in excess of 400 applications. The potential value for archiving portfolio data will vary significantly from one application to another. HPES recommends conducting a pilot effort on one of the County's applications to validate the potential for reducing application data storage requirements rather than starting with a County-wide implementation of Portfolio Application Archiving.

Previously, the County, with the support of HPES, identified Treasurer-Tax Collector (TTC) CRS as a candidate for the pilot effort. Following the pilot, we would work with the County to develop a strategy and roadmap for extending application data archiving to other County applications.

- Automated Tools – Automated systems and tools involved in proposed solution

We propose using the SDM tool, described above, to reduce the data footprint of the County's structured data. SDM software comprises an integrated set of components that facilitate design, deployment, and ongoing management of archiving processes throughout the lifecycle of applications and data. In addition, they deliver capabilities that address different levels of application complexity, data volumes, and archive access requirements. The components include the following:

- Designer – Provides a visual interface to model data and create business-aligned data migration rules with ease
- Data movement – Makes sure data relocation is performed to meet volume requirements while retaining application integrity at all times
- Archive access – Provides a full range of access capabilities to meet requirements for business operations, regulatory compliance, and legal discovery
- Job engine – Automates all archiving tasks with built-in recovery and restart
- Management console – Provides system configuration, job monitoring, job launching, and complete audit trail capabilities

- Qualifications and Experience – Background and experience in comparable environments

HPES has proven experience providing these types of services to a variety of clients with environments similar to that of the County, as described below.

Leading Pharmaceutical Manufacturer: Solution Description: For the last 4 years, one of the world's leading pharmaceutical groups has been cutting costs. One of its key targets has been to reduce the number of IT applications from around 5,000 to 1,500 to lessen associated complexity, costs, and legal risks. A further issue was that the existing Information Lifecycle Management (ILM) Data Archive did not meet Government regulations, creating a high level of organizational risk. Finally, they were storing more information than required, and system interruptions were commonplace—especially if the company sought to simultaneously extract and purge data. In July 2015, the company purchased HPE Structured Data Manager (SDM) to accelerate the archiving of structured data from legacy applications. The company plans to use SDM on an enterprise-wide basis to decommission 300 applications in 2015 (66 of which require structured data archiving) and 896 in 2016 and 2017 (135 structured).

Client Challenges/Need:

- Meet Government requirements for information governance
- Reduce application and data complexity to reduce risk and lower cost

Client Benefits:

- Significant cost savings through reduction in software licensing
- Automatic migration of data with a complete and documented chain of custody
- Improved data quality during data migration, thereby reducing the risk of future litigation
- Data stored in common record formats
- Consolidation of all data in a standard archive rather than disparate locations.

- Key Considerations and Potential Alternative Approaches

Hyperconverged Integrated Systems: Hyperconverged infrastructure is designed to simplify the design and management of the computing environment by merging and pre-packaging the server, network, and storage components of infrastructure into pre-sized building blocks. To deliver the most value, hyperconverged systems would have to comprise nearly all of the infrastructure deployed in the data center; otherwise, the hyperconverged solution becomes just another platform that has to be integrated

and adapted to existing standards; this would increase rather than decrease overall complexity in the environment.

One possible application of hyperconvergence that the County could consider in the shorter term would be the implementation of hyperconverged infrastructure for servers deployed in County field sites. As systems come up for refresh, we will compare available options in the marketplace for cost, compatibility with established management tools and fielded applications, and if a hyperconverged solution would yield benefits to the County, we will recommend its implementation.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

As described in Section 2.9, Application Infrastructure Services, in response to Schedule 4.3, Section 6.7, HPES will implement Helion MPC and Helion Managed Cloud Broker (HMCB) during the Transition as we build the County's on-demand Dev/Test and Production environments as part of the data center consolidation. These platforms start the County on a path of greater standardization in the virtual/converged infrastructure environment. By implementing a private cloud with standard-sized building blocks of virtual infrastructure, we will be able to test and validate whether a hyperconverged infrastructure will ultimately yield benefits for the County.

When the County is ready for hyperconvergence, HPES will provide the technology partnership to achieve this. If we are able to fully standardize over time on the x86 platform in the converged infrastructure, then the next logical step is to plan, design, and implement a hyperconverged infrastructure. During the planning phase we will build the business case for hyperconvergence and will provide the County with alternative solution designs built on the most suitable and current technology and vendors available. HPE offers a wide range of hyperconverged systems that we continue to advance and innovate with to suit various business cases and client needs.

To achieve the best possible outcomes from the County's investment in this technology and to meet its needs in a way that helps to better support County business, we will consider and evaluate the following features to help the County select the optimal hyperconverged solution:

- **Integration for Seamless Coexistence**. Ability of the hyperconverged solution to integrate with the legacy environment. The hyperconverged solution must enable the County to fully integrate the new solution with the legacy environment. Existing server and storage assets must be able to coexist with the new environment until the eventual collapse of multiple administrative interfaces into fewer simpler tools.
- **Scalability**. Ability to grow the environment in a nondisruptive manner and the ability to scale up or scale out without replacing the initial equipment with new equipment. The solution must offer just-in-time growth capability to avoid the need to carry expensive inventory. Additionally, granularity in scalability is important to scale only the resources required in the increments that make sense for the County.
- **Data Mobility**. Ability to move data around to accommodate individual device outages—the ability to easily move data between the hyperconverged platform and other systems, without having to rely on consultants.
- **Data Protection**. Ability to protect data in the event of hardware failures, human error, or natural and manmade disasters while meeting desired SLAs, RPOs, and RTOs without the need for an additional software or hardware layer. Features we will evaluate for the County include RAID or mirroring, fault tolerance, replication (synchronous and asynchronous) within the site and between sites as well as full disaster recovery capabilities.
- **Performance**. Ability to provide performance opportunities that are considered enterprise-class. This means that the solution should support flash and, optionally, spinning disk. Ideally, both will be

supported because they have different strengths and weaknesses. When it makes sense, the solution should be able to automatically tier storage systems to enable faster data access or, at the very least, have an accelerated method for handling data retrieval.
- **Availability**. Ability to provide availability at SLA levels that meet County requirements for all systems. To determine this, we will evaluate ease of scalability, ease of management, ability to scale out storage, tolerance for node loss, cluster resiliency, and capabilities of automated failover.

Once we have identified and received County approval of the plan, in a parallel but fully integrated mode of operation we will execute a phased migration of the County's systems to the new hyperconverged infrastructure. Our plan will also consider data center component refresh dates to maximize investments in the legacy environment prior to the migration.

Timing: Preparation for implementation of a hyperconverged infrastructure will occur during transition. HPES recommends the actual implementation to occur as data center components come up for refresh.

Risk: None at this time.

Dependencies and Milestones:

- Prior to the County investing in a hyperconverged integrated solution, standardization on the proposed Managed Private Cloud platform must be established
- To migrate to a hyperconverged infrastructure, existing legacy equipment will need to be refreshed onto the hyperconverged platform.
- Development of implementation strategy and plan.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

With the implementation of hyperconverged systems, methodologies and process for deployment become easier as a result of the pre-configuration of server, network, and storage components of infrastructure into pre-sized building blocks. These systems include easy-to-use management tools designed to streamline implementation and management and help shield the administrator from much of the underlying architectural complexity.

Our new HPES hyperconverged systems deploy VMs in just five clicks, update hardware and firmware in just three clicks, and provide instant diagnostics and analytics to enable faster response to business needs.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

HPES' facility approach is to deploy the new hyperconverged infrastructure at our primary data center in Tulsa, Oklahoma and/or in field sites as deemed appropriate.

- Automated Tools – Automated systems and tools involved in proposed solution

Our vision is to dramatically simplify and streamline IT administration and operations management. While many hyperconverged integrated system solutions are available on the market today, HPES is a market leader in hyperconverged systems. Our hyperconverged systems offer an infrastructure that provides the following features/benefits:

- Rapid provisioning of VMs
- Flexibility and speed to add capacity in as little as 15 minutes
- Simple IT operations with firmware and driver updates in just three clicks
- 99.999% continuous data availability
- Federated lifecycle management
- Data fabric with data mobility across systems, sites, and cloud

- Lower startup cost with two-node entry and linear scaling
- 62% lower cost for disaster recovery
- Pay-as-you-grow flexible capacity model

Using HPE OneView as the common software-defined convergence platform, we provide software-defined management for both our larger ConvergedSystem 700 powered by Intel models as well as the smaller CS200-HC models. The HPE OneView user experience (UX) makes managing and monitoring systems so easy, no manual is required. HPE OneView integrates with HPE Helion OpenStack and CloudSystem and has extensions to a variety of management software. With a commitment to provide clients with the most flexibility, we have been continually and significantly expanding this ecosystem since 2015.

- Qualifications and Experience – Background and experience in comparable environments

Uniting market-leading HPE Converged Infrastructure with decades of experience in solution design, HPES delivers the ConvergedSystem Portfolio—offering a purpose-built system that dramatically simplifies IT.

HPE ConvergedSystem delivers components designed from the start for convergence, coupled with integrated OneView management and workload optimization based on decades of expertise. The result—a single holistic computing ecosystem.

HPES has proven experience providing hyperconverged integrated systems and services to a variety of clients with environments similar to that of the County, as described below.

City of Los Angeles Department of Building and Safety: Solution Description: The City of Los Angeles Department of Building and Safety Technology Services Bureau supports 1,100 employees to perform permitting, inspection, and code enforcement. The Department processes an average of 120,000 permits per year and provides management for application projects. In the last 12 months leading up to the HPES Converged Systems solution, the client reported two major outages preventing hundreds of customers from doing their work, hurting their reputation as well as the construction industry and economy in general.

Client Challenges/Needs: The client reported frequent hardware failures, power failures, and struggles with keeping systems cool in the space-confined communication rooms and closets hosting equipment in their district offices. The client also struggled with high maintenance costs and frequent travel to remote sites to perform maintenance tasks. They needed to save costs and time, while improving availability.

Client Benefits: We provided a scalable hyperconverged solution within a single box in district offices to provide the services they needed. End users reported a 30% improvement in performance. Provisioning went from weeks to less than a day. They went from two full racks of equipment per site to two units of a single rack. The HPE hyperconverged system boxes, which generate no heat, reduced power consumption and cooling costs. We also reduced travel costs with remote management and low maintenance. The client had a single interface to perform remote management using HPE OneView, slashing maintenance costs. No outages were reported since we implemented our hyperconverged solution. With this scalable solution, the client can add more applications and storage as needed.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

Initiative: E911 (Exhibit KK, Section 3.7)

- Key Considerations and Potential Alternative Approaches

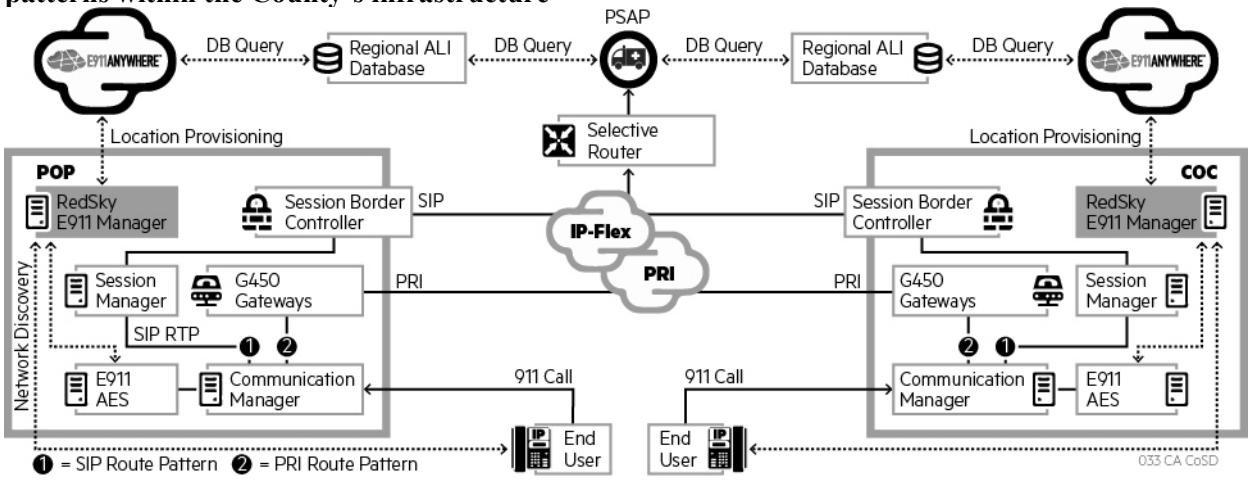
Enhanced 911 (E911) is an important complementary solution to an enterprise Voice over Internet Protocol (VoIP) deployment. As call control is converged into the geo-redundant voice core infrastructure and VoIP is enabled at the telephone set, there is an imperative to provide emergency responders with accurate and detailed information about the source and location of the caller. We propose integrating a site-by-site deployment of E911 services in conjunction with the VoIP upgrade activities proposed in the Voice Transformation response.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

The solution highlighted in this section specifies the E-911 migration planned for implementation early in the contract at existing VoIP sites and ongoing in parallel with VoIP site upgrades. AT&T believes this implementation is crucial to the voice services described in Section 4.3 of the RFP and is priced in Exhibit 16.1-1 accordingly.

HPES recommends the adoption of the industry leading E911 Manager and E911 Anywhere by RedSky technologies. RedSky's E911 Manager® solution will be implemented in line with the County's geo-redundant network core, with infrastructure at the AT&T Point of Presence (POP) and the County Operations Center (COC). The primary application will run on an active host with a standby host that will take over in the event of failure of the primary server, enabling full redundancy.

Figure 187. Fully-integrated E911 solution will automate the E911 process by recognizing route patterns within the County's infrastructure



The E911 Manager will automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager via the AT&T MPLS network to track and update phone moves, adds and changes.

To handle the growing deployment of VoIP services throughout the County, RedSky's E911 Manager will communicate with the Avaya Enterprise voice network to monitor registration events of VoIP endpoints. E911 Manager will use Layer 2 Network Discovery or Layer 3 Network Regions to determine the location of the user based on port, network device, or IP address and will update the Avaya Communication Managers with the proper Emergency Line Identification Number (ELIN) for 9-1-1 off-net calling. The E911 Manager server will create and store Automatic Location Identification (ALI)

records as necessary and submit to RedSky's E911 Anywhere® cloud service in the required format for the local Public Safety Answering Point (PSAP).

To manage ALI information centrally—for County locations or to support mobile softphone users—the proposed RedSky solution includes RedSky E911 Anywhere cloud service. E911 Anywhere is a cloud-based 9-1-1 call routing service that can connect a 9-1-1 call to more than 6,000 PSAPs in the USA and Canada. E911 Anywhere is an effective choice for the County based on its distributed locations as well as the increase in mobile and desktop IP softphone users. The recommended solution by AT&T will feature the following:

- A fully automated E911 solution that will track the location of phones as phones move within the County's enterprise voice network
- An E911 software application located at the AT&T IDC and COC that will interface with the Geo-Redundant Avaya Communication Manager voice network
- A solution that connects with all Private Switch-Automatic Location (PS-ALI) Identification databases throughout the cities within the County
- A solution that provides Emergency On-Site notification to anyone working at the County of the location of a call placed to 9-1-1
- Geo-Redundant Active / Active Server construct located at the AT&T Internet Data Center (IDC) and COC for high availability and redundancy
- Reporting and metrics for auditing of all E911 activity
- As a "cloud-based" 9-1-1 call routing service, E911 Anywhere can send a 9-1-1 call to any PSAP in the U.S. or Canada (with County approval)

E911 is a necessity for the County enterprise VoIP deployment. As stated in the introduction, this solution will be integrated into the County's enterprise-wide VoIP migration, enabling functionality on a site-by-site basis over the length of the transformation initiative.

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

For the proposed e911 solution, AT&T will leverage the local LCM (Life Cycle Management) team, in-house vendors, direct manufacturers, and carriers. AT&T personnel will provide this support from its location on Trade Street in San Diego.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

All support services—whether triage, new requests, change requests, or removals—are initiated by the County user to the HPES Service Desk. All requests within the network framework for E911services will be directed to the AT&T LCM team for assessment and completion.

AT&T will leverage the RedSky's solution for updates to the PSAP routing and PS-ALI databases as County staff request Adds, Moves or Changes to their VoIP telephone stations. The tracking of VoIP phones is made possible by enabling Layer 3 Network Regions on the County's LAN. This is the most common method of tracking IP, SIP, and IP soft phones inside an enterprise. This method, which is specific to Network Regions or subnets, establishes a dedicated block of IP addresses associated to the region at the DHCP server. Each Network Region will then have assigned to it a physical address and an ELIN. Every time a VoIP phone registers to the Avaya Call Manager at the AT&T POP or County Operations Center, E911 Manager reviews the IP address of the VoIP phone to determine if the IP address falls into one of the IP address ranges set aside for the regions. If E911 Manager determines that a VoIP phone is in a Network Region, E911 Manager will provide the ELIN to the respective Avaya Communication Manager server at the AT&T POP or County Operations Center.

- Automated Tools – Automated systems and tools involved in proposed solution

E911 Manager solution will automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T Multiprotocol Label Switching (MPLS) network to track and update VoIP, digital, and analog phone moves, adds, and changes.

E911 Anywhere is a cloud-based 9-1-1 call routing service that can connect a 9-1-1 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada.

- Qualifications and Experience – Background and experience in comparable environments

RedSky is the leading provider of on premise and cloud-based E911 solutions. More than a million workers, students, guests, and visitors use RedSky for E911 protection. RedSky leverages legacy standards as well as the new National Emergency Number Association (NENA) i3 standards for Next Generation 9-1-1 (NG9-1-1) to help organizations provide effective 9-1-1 emergency response, comply with state E911 regulations, and meet business requirements for safety, risk management, and efficiency.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

With our E911 solution, emergency responders will receive information for the building location including the floor of the building from which the call was placed. An alternative approach is to define the PSAP information all the way down to the office/cubicle for the caller; this is not included in the proposed solution.

Initiative: Identity Federated Services (Exhibit KK, Section 3.8)

- Key Considerations and Potential Alternative Approaches

HPES took into consideration the following items, in addition to those identified in the RFP, in making the decision to recommend retaining the current identity and access management (IDAM) platform that the County uses and expanding it to enable the Identity Federated Services through the addition of HPE Identity and Access Management as a Service (IAMaaS). We decided on this solution because it offers the following benefits:

- Low risk to the County
- Speed of implementation
- Low risk to County business partners
- Ease of use
- Leverage existing infrastructure and licenses for County's Oracle IDAM platform
- Existing knowledgebase within the County' and HPES technical and architectural teams
- Maximizes the County's current investment

Potential Alternative Approaches: HPES considered full implementation of HPE Identity and Access Management as a Service (IAMaaS), which would provide identity management of internal as well as external users such as citizens. We decided against this solution because it would require removal of the County's current Oracle IDAM solution, which does not protect the County's investment in the current platform and introduces risk.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

HPES analyzed Okta, Oracle, and IAMaaS during the technology selection stage and recommended HPE's IAMaaS due to the maturity of the product and services, purchase and maintenance cost, and lower risk during implementation. However, if the County opts for another solution such as Okta or Oracle, HPES will work with the County to plan and execute a successful implementation of either vendor's solution.

The recommended Identity Federated Services solution includes the following components:

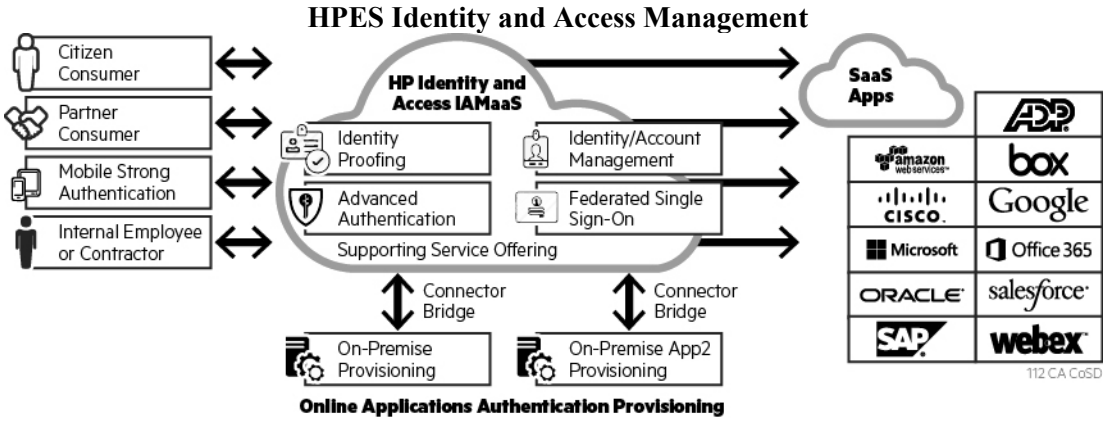
- The existing Oracle IDAM technology platform as its core
- Microsoft Active Directory Federation Services (ADFS)
- HPE's IAMaaS to enable the federation services where the County is acting as service provider and identity provider.

The first two components of the solution are discussed fully in Section 2.5.13 (response to Schedule 4.3, Section 2.18). The remainder of this section describes IAMaaS solution. HPES will use IAMaaS to integrate external constituents within the County's Identity Management Service. IAMaaS is a cloud-based IDAM) solution built using the Computer Associates (CA) secure cloud product for multi-tenancy. IAMaaS is hosted on the HPE Helion Managed Virtual Private Cloud for U.S. Public Sector. The following elements describe the main features of the IAMaaS solution and how they relate to the County:

- User life cycle management such as self-registration, password resets, and profile updates.
- Application access management to request access to applications.
- Hybrid provisioning cloud and on premise to create/update on premise identity requirements.
- Identity synchronization on premise to make certain that relevant data is updated one way or bi-directionally.
- Reporting for compliance and audit.
- Identity proofing from the solution to County data stores.
- The single sign-on (SSO) Federation Hub can act as identity provider (IDP) and service provider (SP) to County software as a service (SaaS) applications.
- IAMaaS can act as a Federation Hub. External users can be authenticated to SaaS apps using their County/IAMaaS credentials, County credentials, or social login credentials like Facebook.
- The CA Security SaaS Validation Program helps SaaS vendors increase sales and adoption by simplifying and validating their SSO interoperability. It enables smooth integration of SaaS solutions into CA SSO environments in a user-friendly and cost-effective way.
- Credentials may include Forms, Integrated Windows Authentication (IWA), multi-factor authentication (MFA), public key infrastructure (PKI), Radius, OAuth, one-time password (OTP), and Risk.

Figure 188 illustrates the main elements of the IAMaaS solution and its relationship with the County, its citizens, employees, and partners. On the left side is each type of user who will interact with the service. Within the core or "cloud" of IAMaaS are the key services provided such as identity proofing, identity and account management, federated SSO, and advanced authentication. The resources and services to access are on the right; those services are both internal and external to the County IT environment, including third-party providers. Connectivity to the resources via the IAMaaS are enabled via industry-standard IDAM protocols.

Figure 188. IAMaaS solution



Providing secure IT services operations through robust user identity authentication.

Rationale: We believe that expanding the current IDAM capability along with implementation of HPE's IAMaaS for identity management of external users provides the most cost-effective solution. This approach *provides a low risk, non-disruptive method* to expand on existing County investments and meets the County's architecture vision for identity management.

Timing: The timing for expansion of the existing County IDAM solution to include federation will coincide with the ConnectWell San Diego project or other timing as required by the County. Other elements of the solution such as federation requests to business partners will occur as the solution is deployed.

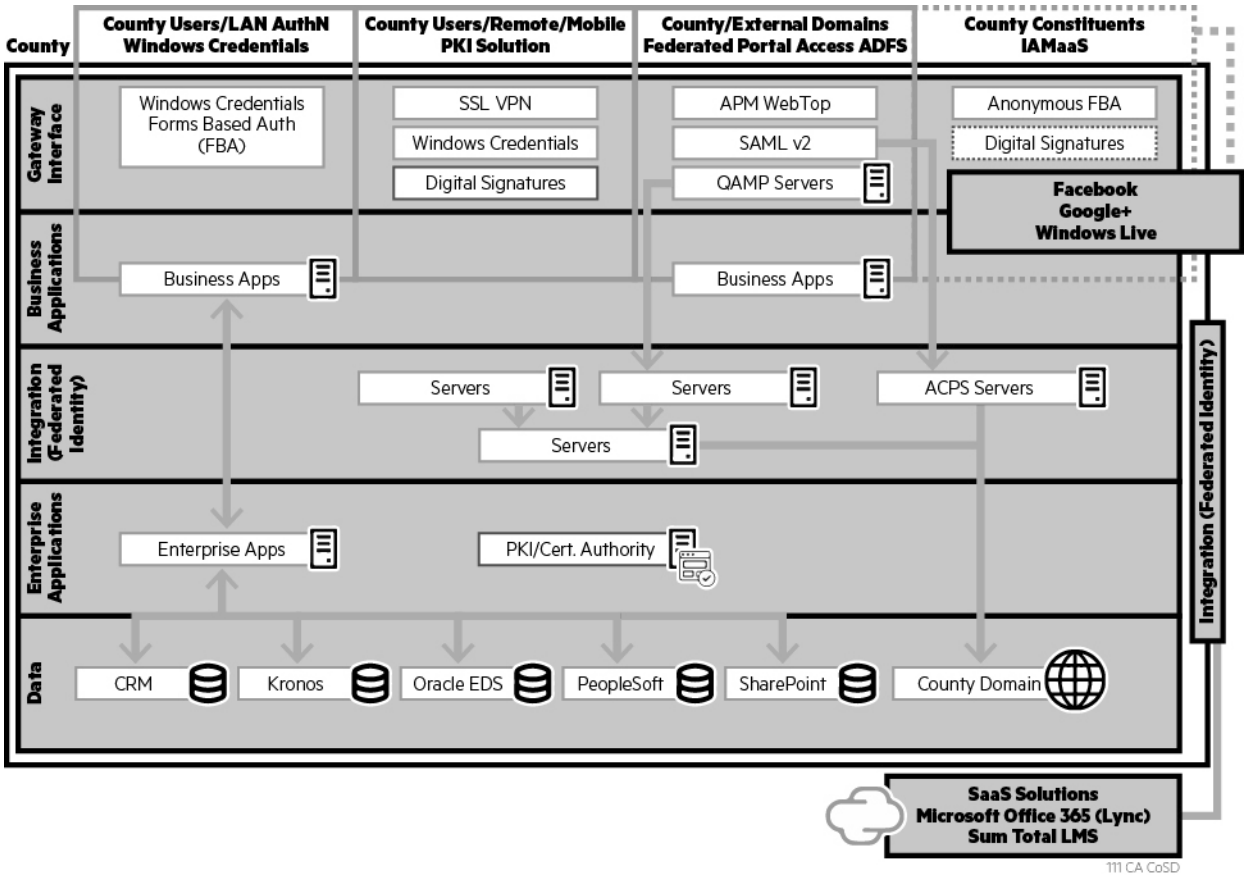
Figure 189 below depicts the overall view of the IDAM solution and how Oracle, ADFS, and the HPE's IAMaaS will work together to provide identity federation. As seen in the figure, the core elements of the IDAM solution will work together to enable seamless federation between the County and third-party providers, external State and Federal agencies, and identity management for County residents.

The County ADFS 2.0 environment—a key component of the Identity Federated Services—has been operational since 2011, providing secured identity federation and web SSO capabilities for County and external business unit end users who require access ADFS-secured applications within the County network and in the cloud.

Earlier in 2016, the ADFS environment was upgraded to v3.0 with redundancy, and included a new test environment. By adding external access to the test ADFS server, this upgrade provides expanded use of the ADFS test environment for development and testing of new ADFS-secured applications.

Upgrading the ADFS environment was part of the County's overall IT roadmap to refresh and improve key infrastructure components and expand the County's IDAM solution. The key point is that this solution is strongly tied to the Identity and Access Management Services solution; it is a continuation of that capability but expanded to enable federation—much of the approach is duplicative.

Figure 189. The proposed new IDAM solution integrates Oracle, ADFS, and the HPE's IAMaaS



This solution offers minimal risk to the County and enables seamless federation between the County and third-party providers, external State and Federal agencies, and identity management for County residents.

Key Dependencies and Milestones: As a part of the overall IDAM effort, Identity Federated Services is encapsulated in the following list, which details the progressive steps of the IDAM solution and details what is being done today and what HPES will perform in the future:

- Current/on-going effort – Oracle Federation Manager is currently deployed with Service Provider active and Identity Provider not active. Based on an existing request from the Department of Child Support Services (DCSS), we plan to implement the Federation Acting as Identity Provider upon approval. To deliver the federation capability for DCSS, IAMaaS needs to be implemented simultaneously with Federation Acting as Identity Provider.
- Future – Develop a process for auto-onboarding new employees based on the information in PeopleSoft to create the Active Directory (AD) identities
- Future – Expand use of the existing platforms into all County business units and partners as well as work with the current Knowledge Integration Project (KIP) team (IBM) to expand to partners
- Future – Use HPES IAMaaS solution to expand to County residents and to act as the identity manager for County residents
- Future – Re-architect the solution to become a zero downtime solution
- Future – Federate with County third-party vendor applications

- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

Ongoing support for the IDAM service will be delivered by continental U.S.-based delivery resources in line with the County's requirements. With more than 5,000 security professionals who have IDAM expertise, HPES has the experience to deliver even the most complex solutions.

The HPES Tulsa Data Center will be the production data center, with the IDAM solution delivered from this location. This includes almost all web, application, and database servers, data storage, and data management. The HPES disaster recovery (DR) site in Colorado Springs will provide the recovery site for the IDAM solution.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

HPES will adhere to the following key processes to deliver Identity Federated Services:

Solution Methodology: By incorporating the HPES IT Strategy & Architecture (ITSA) for Identity Federated Services, we will take the same iterative approach, addressing issues and improvements in data quality and data management—in both practice and implementation. Through this process, HPES will work closely with County data teams and other HPES Transformation, Integration, and Architecture (TIA) data architects to define and manage County IT outsourcing enterprise data semantics. ITSA for Identity Management advocates a rapid, incremental, and iterative approach that can be aligned with the County's hybrid development methodology.

In addition to the ITSA, we will use standard TOGAF (The Open Group Architecture Framework)-based architecture approach to develop the solution artifacts and produce the required documentation to make certain that the solution is documented correctly and that it also will lower the overall implementation risk to County. We will integrate these key methodologies with the County's current Architecture and Solution reviews in conjunction with the County Technology Office (CTO) and relevant County groups.

For the Oracle IDAM Suite, HPES will work with our IDAM architect to make certain that the design, development, and deployment of the Oracle suite follow standard Oracle design and deployment methods. This will facilitate operation of the Oracle platform within the design parameters. Any significant design changes to the platform or changes to the Oracle databases will follow Oracle mandated practices.

- Automated Tools– Automated systems and tools involved in proposed solution

HPES will use the Oracle and Microsoft tools identified in Table 87. in support of Identity Federated Services.

Table 87. Automated Tools for Support of Identity Federated Services

TOOL	PURPOSE
Identity Manager	• Oracle Identity Manager is designed to manage user access privileges across all of the County's resources, throughout the entire identity management lifecycle—from initial creation of access privileges to dynamically adapting to changes in business requirements. Identity Manager enables the incorporation of necessary business changes at minimal cost, while avoiding enforced customization.
Access Manager	• Oracle Access Manager provides adaptive authentication, federated single sign-on (SSO), risk analysis, and fine-grained authorization extended to mobile clients and mobile applications. Services can be licensed and enabled as required to meet the specific needs of the County.

TOOL	PURPOSE
Federation Manager	• Oracle Identity Federation (OIF) provides secure identity information exchange between external/internal partners. OIF provides account management for partner identities and integrations through support of industry federation standards. OIF protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers, and applications.
Virtual Directory, Unified Directory	• Oracle Virtual Directory provides Internet and industry-standard Lightweight Directory Access Protocol (LDAP) and eXtensible Markup Language (XML) views of existing enterprise identity information without synchronizing or moving data from its native locations.
Microsoft tools and services also be used: • Microsoft Active Directory 2012 • Microsoft ADFS	• Microsoft Active Directory (2012) Domain Services (AD DS) provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications. Administrators can use AD DS to organize elements of a network—such as users, computers, and other devices—into a hierarchical containment structure. The hierarchical containment structure includes the AD forest, domains in the forest, and organizational units (OUs) in each domain. • ADFS (Active Directory Federated Services) provide County users with SSO access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and to implement federated identity. (Claims-based authentication involves authenticating a user based on a set of claims about that user's identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the user by other means, and that is trusted by the entity doing the claims-based authentication.) It is part of the AD DS.

- Qualifications and Experience – Background and experience in comparable environments

HPES has experience delivering IDAM services that include the following:

- Managing 59 million usernames and passwords
- Managing and monitoring more than 6,000 firewalls
- Executing 3,000 IDs for threats and vulnerabilities
- Completing more than 250 custom security audits annually
- Providing laptop and desktop encryption in 65 countries for more than 575,000 devices

Additionally, we provide similar services to a variety of clients in an environment comparable to that of the County, as described below.

County of San Diego: HPES has successfully deployed all of the major Identity Management elements currently running within the County of San Diego including Active Directory (AD), Active Directory Federation Services (ADFS), Oracle Identity Management Suite, Public Key Infrastructure (PKI), Office 365, and Digital Signatures. This includes continuing integration and design efforts.

U.S. Navy Next Generation Enterprise Network (NGEN) Program: HPES currently manages a full-spectrum identity management and lifecycle capability for the United States Navy that encompasses the entire United States land-based Naval and Civilian services including both unclassified and classified domains. We manage more than 800,000 user identities across the two environments, which encompass

human resources (HR), support, healthcare, and third-party systems. HPES works directly with the Navy customer to institute business and process rules into the IDAM capability.

Massachusetts Executive Office of Health and Human Services (EOHHS), Massachusetts Medicaid Management Information System (MMIS): HPES designed, developed, implemented, and now maintains and enhances the MMIS system for Massachusetts. HPES replaced the previous, state-operated Medicaid system with the new Web-based, service oriented architecture (SOA) application constructed to integrate into the state's enterprise SOA infrastructure. The infrastructure includes shared services such as enterprise identity management and electronic payments. The MMIS has enabled the consolidation of health data and enabled the timely implementation of new policies and programs.

The MMIS applications are integrated via Web services with enterprise access management systems to enable user SSO. Self-service user ID management features were developed and implemented for the new Provider Online Service Center (POSC) Web site. These features allow the primary user ID for a healthcare practice or hospital to create and administer user IDs for their own staff, rather than calling a help desk. An online security administration subsystem was developed to provide EOHHS security staff the ability to administer role-based authorization for both internal and external users. The MMIS system uses digital certificates to secure service-based interfaces with internal and external systems. During implementation, HPES issued new cards to 1.1 million members and provided a self-registration feature to create new user IDs for 24,000 active providers.

Hirschvogel Automotive Group: For this client, HPES created and implemented an HPE identity management solution that integrates SAP NetWeaver Identity Management with SAP HR, SAP ERP, and Active Directory residing in various business units and locations. HPES led the company in all project phases, including project management, solution design, and implementation. HPES now supports the company in maintaining and developing the identity management solution.

The new identity management solution is designed to make available high-quality personal data in a secure central identity management (IDM) system. It minimizes manual administration and limits access to personnel information.

In workshops with HR and IT staff, HPES helped Hirschvogel analyze its identity management requirements and develop a set of specifications. Based on these, the HPES team created an HPE Identity Management System and implemented it with SAP NetWeaver Identity Management to the following requirements:

- Build a reliable identity provisioning infrastructure
- Integrate the system very tightly with the company's HR processes—partial relocation of staff workflow in the Identity Management System
- Create a central workflow engine to implement management processes
- Delegate administration of user privileges
- Establish a central review point for all activities involving managing users and permissions
- Connect SAP HR
- Connect various Active Directory domains within the company
- Connect SAP ERP

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

HPES considered an alternative approach, as described above in the Key Considerations and Potential Alternative Approaches section.

Alternative Approaches – Other Proposed Initiatives (Exhibit KK, Section 4)

HPES proposes two additional transformation projects for consideration by the County described below.

Enterprise Information Management

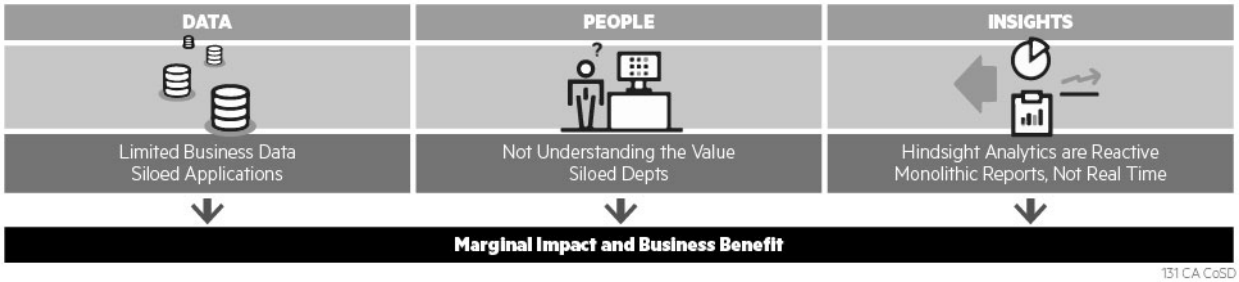
- Key Considerations and Potential Alternative Approaches

HPES recommends implementation of an Enterprise Information Management (EIM) program to capitalize on the valuable data that is available but currently not harnessed. This will provide the County with information it needs to make more informed decisions and present an enterprise view of the data that could be used to make richer programs available to the public.

The County has begun the journey to modernize the Information Architecture and Governance model a critical step as modernization and transformation of the IT infrastructure begins. The information architecture must address traditional "feeds and speeds," and include business definitions of information and the information processes to incorporate all data (structured, semistructured, and unstructured (xml, flat files, scanner files).

Siloed business data, as shown in Figure 190 makes it difficult to take full advantage of the information available across the enterprise. To the County, this could mean employees are limited in their ability to perform certain job functions or provide the services citizens need. This can result in added frustration for both employees and citzens.

Figure 190. Siloed Business Data



When data is siloed, it is more difficult and time consuming for County employees to find the information needed to support citizens.

EIM provides an essential framework for managing and governing information (data) across the enterprise and requires:

- Governance and stewardship
- Integration
- Methodologies and standards
- Architecture and technologies
- Enterprise data models

The payoff for an EIM solution is clear—the County will be better prepared to more rapidly meet the needs of employees and citizens by gaining greater insight from the data it collects, as shown in Figure 191.

Figure 191. Integrated Data Across the Enterprise.

Easy access to all available data facilitates decision making and helps to achieve superior business outcomes.

As HPES and the County develop a modernized Information Architecture and Governance model, we will consider a wide-range of common challenges that include:

- Inconsistent definitions of key business data, leading to incomplete, incorrect business metrics
- Information that is not available, incomplete, inaccurate, and untimely to enable informed business decision
- Time-consuming, manual processes, adding to employee workload and citizen frustration
- Fragmented data, preventing or delaying comprehensive situational analysis and appropriate actions
- Siloed project work, preventing integration or extension across enterprise
- Inconsistent data, preventing standardization and reuse of processes, methods, among others
- Siloed decision making, which may be counterproductive to the enterprise
- Poor data quality and fragmented data security/auditability, exposing compliance risks (SOXA, HIPAA, ISSA, CCA, FRCP, Basel II Accord, PCI, EU Privacy Directive, etc.)
- Unknown data retention needs/requirements, transforming data assets into data liabilities (storage costs & exposure risks).

HPES recommends EIM for developing a coherent and supportable Information Architecture and Governance model. This approach will focus on developing an information strategy and a roadmap for implementing the strategy, and then to invest in delivering the supporting initiatives.

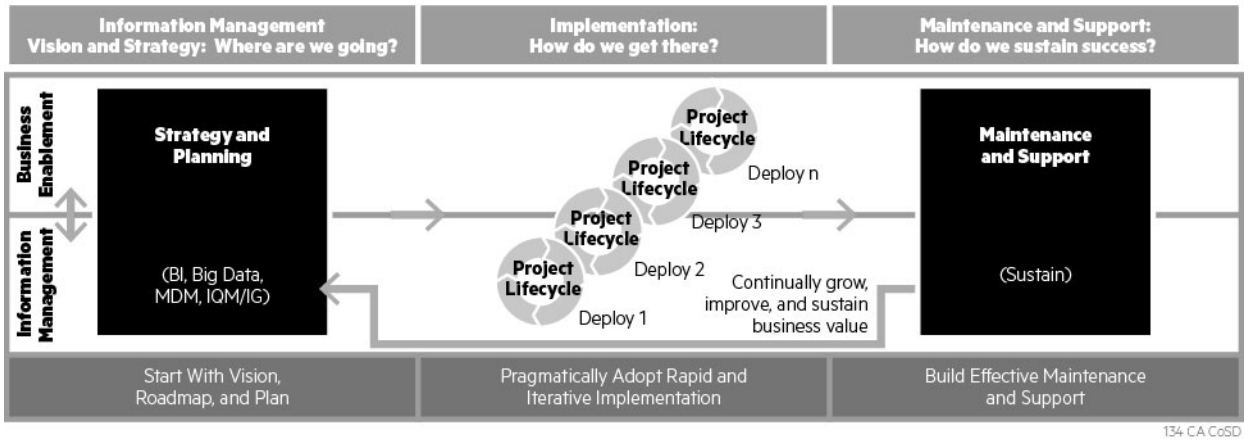
- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

We propose a two-phased approach to establish a coherent EIM program. The first phase is a stand alone project and it is priced as a new capability in Schedule 16.1.1. This project focuses on the objective defining the County's EIM program. Key deliverables from this project include: Vision and Strategy Document and EIM Roadmap.

The second phase is would consist of a number of separate projects detailed in the Roadmap from Phase 1. Each project will have well defined objectives and deliverables defined throughout the implementation process. Specific intitiatives/projects identified in the roadmap are executed in a rapid and iterative approach. HPES scopes the implementation projects upon completion of the vision and strategy. Projects associated with the second phase are not priced in this proposal and would be completed via work request.

Figure 192 illustrates the HPES approach to EIM. Of particular note, our approach is to address and align business enablement with information management.

Figure 192. HPES Approach to EIM



Our approach aligns business enablement and information management that address true business needs.

Rationale: EIM provides the framework for managing and governing information across the enterprise. An EIM program enables data sharing for better decision making and provides County leaders with insight into to the quality of services that they deliver to their citizens.

Timing: We estimate the time required to develop the information management vision and strategy and roadmap to be a 3- to 4- month period that would occur after transition. We will work with the County to determine the business needs and to document the supporting technical requirements. To minimize the County's time investment, while maximizing impact, we will conduct information gathering through a series of focused discussions with stakeholders. This helps us to have an accurate understanding of the current environment as well as the desired future state. At the end of this effort, we will deliver a strategy and roadmap for review and approval by the County.

Risks: None identified.

Dependencies: Developing an effective EIM program is dependent on the active involvement of the business groups as well as the CTO.

Milestones: Key milestones in the planning and implementation of EIM include the following:

- **Milestone 1 – Business Needs Assessment.** A core component of the information gathering phase of the strategy and vision project that focuses on the needs of the business in terms of EIM.
- **Milestone 2 – Current State Assessment.** The second core component of the information gathering phase focuses on documenting the existing technical environment to support EIM
- **Milestone 3 – Desired State Gap Analysis.** The transition step into analysis and planning phase where we document the gaps between what the County's business needs are and the current technical environment.
- **Milestone 4 – Strawman Vision and Roadmap**. This milestone reflects HPES draft strategy and roadmap for the County.
- **Milestone 5 – Final Vision and Roadmap.** Once the County reviews and approves, HPES provides the final strategy and roadmap to guide implementation the of EIM program.

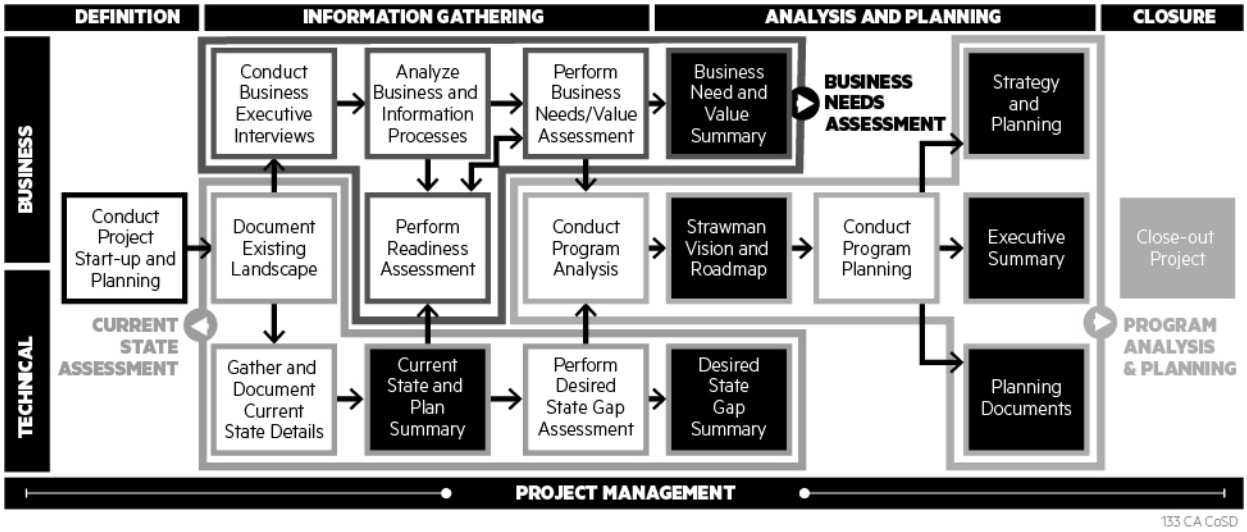
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

For the development of the County's Information Management Strategy, Vision, and the supporting Roadmap, HPES provides a small team of experienced consultants to work on-site in San Diego with the local support team and key County stakeholders.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

During the past 40 years, HPES has developed and documented its IT Solution Architecture (ITSA). This methodology, described in detail in Section 2.5.6 of this proposal. This methodology will provide the foundation for our EIM solution. With Figure 193 identifies the detailed steps for both the development of strategy and vision and implementation.

Figure 193. HPES Global Methods for Information Strategy Master Plan



HPES uses a collaborative approach to identify and document requirements and gain concurrence for the way forward.

The methodology uses a collaborative approach to align business needs with technology by documenting the current state of technology, process and strategy. Through structured information gathering we document the desired state and analyze of this information to identify gaps between the current state and the desired state. We use this information to develop the roadmap to address the gaps. Each step in the framework results in detailed artifacts tailored to the County. Our consultants are trained on the methodology and are experienced in guiding the process, making sure that the County's experience is positive and the results meet their information management needs.

While not included in the proposed initiative, HPES anticipates that after the County develops its EIM strategy and roadmap, there will be a need to support implementation of EIM. HPES has a mature methodology for implementation and is prepared to support the County in this phase. This methodology applies proven templates and suggests industry best practices to gather the correct information needed for successful implementation. We will work with HPES account team and provide our expertise to help guide project implementation as identified in the County roadmap. Common implementation projects address information management/quality, master data management, information governance, enterprise data modeling, and development of enterprise standards.

- Automated Tools – Automated systems and tools involved in proposed solution

The process for planning and implementing EIM projects relies on standardized templates to gather and document requirements. These result in well-defined deliverables that are guided by an extensive set of artifacts and knowledge libraries. HPES will use its existing methodologies and associated processes to develop the strategy and plan. As we assess the current environment and conduct a gap analysis, we document technology requirements for subsequent implementation projects.

- Qualifications and Experience

HPES has delivered EIM to the following clients:

HealthNet Federal Services (HNFS): Tricare is the Health Care Program for the U.S. Department of Defense (DoD). They recognized that a necessary first step in implementing an effective enterprise information strategy was to develop a roadmap and they engaged HPES. We worked collaboratively with HNFS during an 8-week consulting project using the HPE Global Methods master plan methodology to create the strategy roadmap. Following this initial effort, HNFS has executed on a number of the projects defined in the roadmap, with a goal to improve the quality of service for their customers through better use of data and information.

Customer Challenges:

- Needed better insight into current operations to competitively recompete for its contract with Tricare
- Gain greater insight into needs of customers and quality of services through the effective use of quality data
- Achieve a view into future state architectures for HNFS and look for opportunities for alignment and adoption to HealthNet corporate strategic initiatives.

Customer Benefits:

- Business driven roadmap enabled rapid implementation of key EIM projects
- Improved information quality and governance
- Quality of decision making increased through greater insight gained through information.

Pennsylvania Patient Safety Authority (PSA): PSA engaged HPES to conduct a short-duration consulting engagement, where we guided PSA to create an enterprise-wide information strategy and Business Intelligence (BI) Master Plan. This Master Plan included 1- 3- and 5-year roadmaps outlining a plan for addressing foundational environment and data requirements for critical business analytics. Additionally, it developed the advanced analytics environment for addressing 100% of PSA's data, to include not only structured data but also unstructured (text and narrative) data. This included approximately 300 servers with data spanning 5 years, and a total volume of 1 petabyte.

Additionally, HPES implemented specific projects detailed in the roadmap. Specific activities included data profiling (documented values vs. actual values), data cleansing (identify and remove dirty data only), alignment, data de-duplication, survive, transform, validate, augment, translate ontology, model, steward, certify, survive, encrypt, synchronize, distribute, replicate, publish, and audit. Further, we helped document more than 20 KPIs with associated reporting and analytics models.

Customer Challenges:

- Alleviating the manual gathering of information, creating reports, and conducting analyses
- Addressing inconsistent definitions and data governance that inhibits consistent and meaningful reporting
- Creating effective and supportable metrics for measuring business value.

Customer Benefits:

- Improved patient safety due to improved insight driven by better metrics and consistent reporting
- Extended reporting including true business intelligence and an advanced analytics capability.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

None.

Other Proposed Initiative: Comprehensive Applications Threat Analysis (CATA) Service

- Key Considerations and Potential Alternative Approaches

Building in security from the beginning is essential to keeping the County applications out of harm's way. Likewise for existing applications, assessing security requirements and control gaps, and architectural security robustness and resilience, or lack thereof, is essential to reducing the number and severity of vulnerabilities and maximizing the chance that applications are not missing major security requirements or controls. Industry-standard conventional software development may fail to find, fix, and avoid many vulnerabilities introduced in applications development. HPES would apply our extensive knowledge of SDLC and secure development best practices to design and build the County applications. The additional practices described here would avoid, find, and fix far more vulnerabilities than standard development practices, as these approaches are focused on proactive software security quality improvement and increasing software assurance levels.

With the number and complexity of security attacks on the rise, the County would be well-served by a proactive approach to security quality that saves costs and minimizes risk by greatly reducing security requirements and control gaps as well as reducing the number of undiscovered security defects or vulnerabilities.

- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

Our Comprehensive Applications Threat Analysis (CATA) service uses well-established return on investment (ROI) practices for quality improvement. These practices demonstrate that fixing defects after code implementation can be 30 to 100 times more costly than discovering, avoiding, or reducing the severity of defects early, during requirements analysis, architecture, and design. Conventional software development practices discover and fix only a small fraction of security vulnerabilities later in the application development life cycle; CATA enables achievement of a much higher level of assurance with security and lower rework costs. CATA minimizes security-related rework by helping get it right the first time by identifying security issues in higher layers of abstraction of the application (requirements, architecture, design). This can pervasively improve applications security to complement other efforts to address security issues in source code (static) and run-time behavior (dynamic).

Projects: CATA reviews will be conducted on a subset of the County's applications, selected and prioritized according to factors such as County-provided priority, sensitivity/criticality of data managed by application, impact if the application is compromised (confidentiality, integrity, or availability), significance/scope of application updates (especially new requirements, updated architecture, design, transformation/modernization), any available risk characterizations, and other factors agreed to by HPES and the County. Likewise, prioritization criteria and decisions will be made for static security code reviews and applications vulnerability assessment and penetration testing. In cases where a CATA review is conducted, and it is deemed appropriate to conduct a follow-on CATA review on the same application (for instance, above the risk prioritization threshold for CATA reviews, and having another major release

since prior review), a CATA delta review will be conducted, starting with the CATA baseline analysis initially performed or a prior CATA delta review.

Objectives: the identification of security requirements/controls gaps and vulnerability risks, and recommendations to address (close gaps, lower risks) for each security assessment (CATA, static security code review, vulnerability assessment / penetration test) with intent of improving the security of these applications by a prioritized incorporation of the review recommendations.

Deliverables: A prioritized and vetted list of security findings from each of two CATA phases (Security Requirements Gap Analysis; and Architectural Threat Analysis) with project team commitments to address factored into before and after severities. These can be in the form of summary slides (most common form of deliverable), samples of which are shown below in the Methodology & Key Processes section, or longer written reports at the County's option, which include additional explanatory narrative and background on the specific analysis results that contributed to the findings. Findings from code review and vulnerability assessment and penetration testing are in the form of written reports describing findings, along with severities and remediation recommendations.

Pricing for various CATA offerings are included in Exhibit 16.1.1.

- Methodology & Key Processes – Key methodologies and processes in proposed solution

CATA is a two-phase activity—Security Requirements Gap Analysis and Architectural Threat Analysis––that includes interviews with HPES development staff, analysis by HPES staff and tools, and reporting.

The **Security Requirements Gap Analysis** determines security requirements and control gap for deployment of the application in compliance with applicable regulatory frameworks and industry best practices. The gap analysis will establish security control objectives and lay the groundwork for the threat analysis.

During the Security Requirements Gap Analysis phase, HPES will identify relevant sources for security requirements derived from applicable regulatory requirements. We then will establish traceability from the County's regulatory or business environment to a prioritized set of security requirements. From the information we gather through our proprietary templates and stakeholder interviews, we will determine the plans and commitments for addressing these requirements, with special focus on already-designated technical solutions and already-documented security expectations, and the remaining gaps.

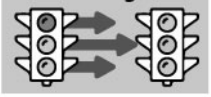
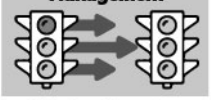
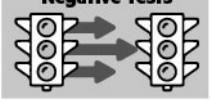
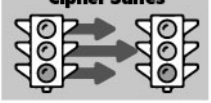
The Security Requirements Gap Analysis is based on:

- Expert system-like templates, with partially encoded expert security knowledge
- Weighted and prioritized input
- Data that is reviewed and calibrated by certified security reviewers
- Efficient, repeatable results
- Requirements traceability from a robust collection of governance sources, including regulations, laws, and best practices.

The end result is a Security Requirements Gap Analysis that will identify important security requirements that may not be met through current plans. It places these at-risk requirements in priority or severity order.

Figure 194 is a sample of summary level Security Requirements Gap Analysis findings, which will be part of a larger findings slide deck.

Figure 194. Security Requirements Gap Analysis Sample Summary of Findings

Remaining Disconnect and Review Progress	Current Release Impact	Future Roadmap
Lacking Least Privilege 	Daemons (Tomcat/JBoss) exposed to internet run with **full-privilege** accounts, **increasing security risks** and potentially increasing security-related **support cost.** Making customer compliance with GLB, BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** **Modify** Tomcat/JBoss (and other **automated processes**) to **run** as restricted users with **least privilege needed.** It may be necessary to do that for Current Release, depending on Threat Analysis results.
Certificate Lifecycle Management 	Supports **only self-signed certificates,** which **require reliance** on **DNS (proven to be unsecure)** and do **not** allow for **revocation verification,** potentially causing **unauthorized access** to customer **credentials.** Making customer compliance with BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** Add **support for CA signed certificates** and certificate **revocation** thru OCSP or CRL verification.
Missing Security Negative Tests 	**No Security Negative Tests** because QA has no experience with negative testing. Making customer compliance with BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** Train QA team on security test tools (e.g., WebInspect) and **include security negative** tests to test plan.
Non-Configurable Cipher Suites 	The **cipher** and **hash algorithms** are **not configurable.** Thus, **customers** may **not** be able to **follow** their **IT policies** and **cannot disable weak algorithms.** Making customer compliance with HIPAA and PCI-DSS difficult.	**Future Release** Make **cipher and hash algorithms configurable.**

173 CA CoSD

This sample report shows an overall security assessment of Medium Risk from non-supported security requirements.

The **Architectural Threat Analysis** is an architecture-level review of the security properties of the underlying components and interfaces and provides recommendations for mitigating all identified moderate- and high-risk areas.

CATA combines information about the target application and deployment environment with target application security plans. An HPES security consultant, uses CATA tools and templates that include a requirements traceability questionnaire and database, and an architectural threat analysis heuristic template. These tools add repeatability, semiautomated risk calculations, and serve as an "additional reviewer in the room." Our security consultant then analyzes the resultant data.

In the Architectural Threat Analysis phase, the CATA team acts as an independent party, and will interview the designated Project Security Architect for the specified application or system. We will then review architecture-level documents to gather information regarding architectural interfaces, components, data, and security characteristics, in addition to security mitigations already planned. HPES has developed a repeatable process that uses a variety of well-established heuristics to identify interfaces and security properties that have the greatest risk of security defects. The HPES analyst will factor in the risk reduction resulting from the mitigations and controls reportedly applied, and identify areas of residual elevated risk as well as technical control opportunities.

The Architectural Threat Analysis invariably finds unnecessarily elevated security risks that would benefit from additional technical controls. HPES investigates specific solutions to address the security risks and provides recommendations based on best fit for the County's organization and mission. This task does not include implementation of the solutions. Architectural Threat Analysis can preempt building security flaws into applications based on the following elements:

- Expert system-like artifacts, encoded with first-order expert security knowledge
- Weighted and prioritized input
- Data that is reviewed and calibrated by certified security reviewers

- Efficient, repeatable results.

Figure 195 is a sample of summary level Architectural Threat Analysis findings (part of a larger findings slide deck).

Figure 195. Sample Architectural Threat Analysis Report

Security Risk Area and Review Progress	Past Behavior	Fix
Least Privilledge	All **process** daemons **running as root** gaining **full access** to the box and **defects can lead to unauthorized** code running as **root**	Create **restricted user** account and use it to **run** the process **daemons**
Support for Third-Party Certificates	Using **self-signed** certificates **hinders** customer **validation, exposing** customer and servers to **man-in-the-middle attacks.**	**Replaced self-signed certificates and provided** means for **validating the certificates** correctly
Full Privilledge Database Account	**Web application using** an admin **root account** was **unneces-sarily** risking to **expose database data**	**Replaced admin** account by **restricted account**
Duplication of Validation Routines	Validation routines were disperse in the code raising the risk of missing bug fixes	**Integrate** in the project a **well-documented** validation **library**
World-Writable Directory	Web application **configuration files** were **world-writable exposing** them to an external **attacker** to be able to **modify important application characteristics**	Included **file system checks** in build **scripts**
Exposed Passwords	Web application and CC service would **leave credit card** information in **clear text** after **freeing memory**	**Wipe memory buffer** before freeing memory

174 CA C65D

The Architectural Threat Analysis prevents security risks from being introduced into application code.

Missing or incomplete security requirements, architectural threats, and/or previously investigated remediation may be identified during the analysis. HPES will report these findings based on their severity: High (Red), Moderate (Yellow), and Low (Green). Severities can be modified if required to match specific regulatory frameworks.

Findings will include a high-level executive summary, slide tables of individual prioritized findings with remediation recommendations, and if a written report is required, a technical discussion section.

While CATA is highly effective for proactively identifying and mitigating potential security risks in the targeted applications, we recommend combining CATA with secure code analysis by a security expert using the Fortify tool or with hybrid combinations such as HPES' human expert security code reviews, in addition to our applications vulnerability assessment and penetration testing. This will result in identifying vulnerabilities through both static and dynamic security analysis, as these highly complement CATA. Static security analysis identifies issues in source code, and dynamic security analysis identifies vulnerabilities in run-time behavior, while CATA identifies security issues in requirements, architecture, and high-level design.

CATA – Complementary Security Services: CATA is a high-level service focused on the requirements and architectural level. Problem areas identified through CATA can often be addressed through other HPES security service offerings. The following additional services help assess whether the security designed in early stages is also implemented correctly:

- **Secure Code Analysis** – Provides validation that the application, once it has been designed correctly, is implemented as designed. This may be a combination of human expert security code review and automated static scanning, such as with HPE Fortify.
- **Applications Vulnerability Assessment** – Provides a further layer of validation that once the application is implemented as designed, known attack vectors do not "break" it. Vulnerability assessment can be performed not only prior to deployment, but also throughout the production lifetime of the application. The assessment can catch some emerging or "zero day" problems with applications that have already been deployed to the field.
- **Penetration Testing** – Penetrates beyond vulnerability assessment to test vulnerabilities discovered in vulnerability assessment for exploitability.

- Automated Tools – Automated systems and tools involved in proposed solution

HPE Fortify on Demand, CATA tools and templates, referenced above. Note that HPE Fortify is distinct from CATA, which analyzes analyses security requirements, architecture, and high-level design, and is human methodology, whereas Fortify is a product/tool to scan code statically (for instance Fortify SCA) and dynamically (WebInspect). These tools are highly complementary, and when used in combination with human expert and hybrid Secure Code Analysis and application vulnerability assessment and penetration testing, they cover security across all major aspects of the SDLC.

- Qualifications and Experience

CATA employs a mature approach with a long history of success. HPES has conducted CATA reviews hundreds of times during the past decade and the results have helped clients to avoid the impact of thousands of vulnerabilities. This service is also enhanced by the following HPES applications security capabilities and professionals:

- Global network of 10 strategically placed HPE Security Operations Centers (SOCs) for monitoring, management, and threat remediation, 24x7x365
- HPES' cybersecurity capabilities cover 67 countries across all industry verticals
- 5,000+ security professionals who manage more than 10,000 enterprise clients
- Greater than 75% of the world's financial companies use HPES services and products
- Tracks billions of security events monthly, securing 1.8+ million devices and 47+ million users
- Manages and monitors more than 6,000 firewalls and 3,000 intrusion detection systems
- More than 800 local, state, and Federal agencies in the U.S. who HPE security services
- Combined security intelligence based on 4 million+ virtual machine sensors and 100,000+ hours of incident response per year.

- Assumptions – Any material assumptions involved with proposed solution, e.g., proposed leverage of current assets, required involvement of County resources beyond what is described in this RFP.

None.

- Alternative Approaches (*optional*) – Submit a description of an alternative approach if you believe it is worth consideration by the County, including rationale, trade-offs and potential benefits.

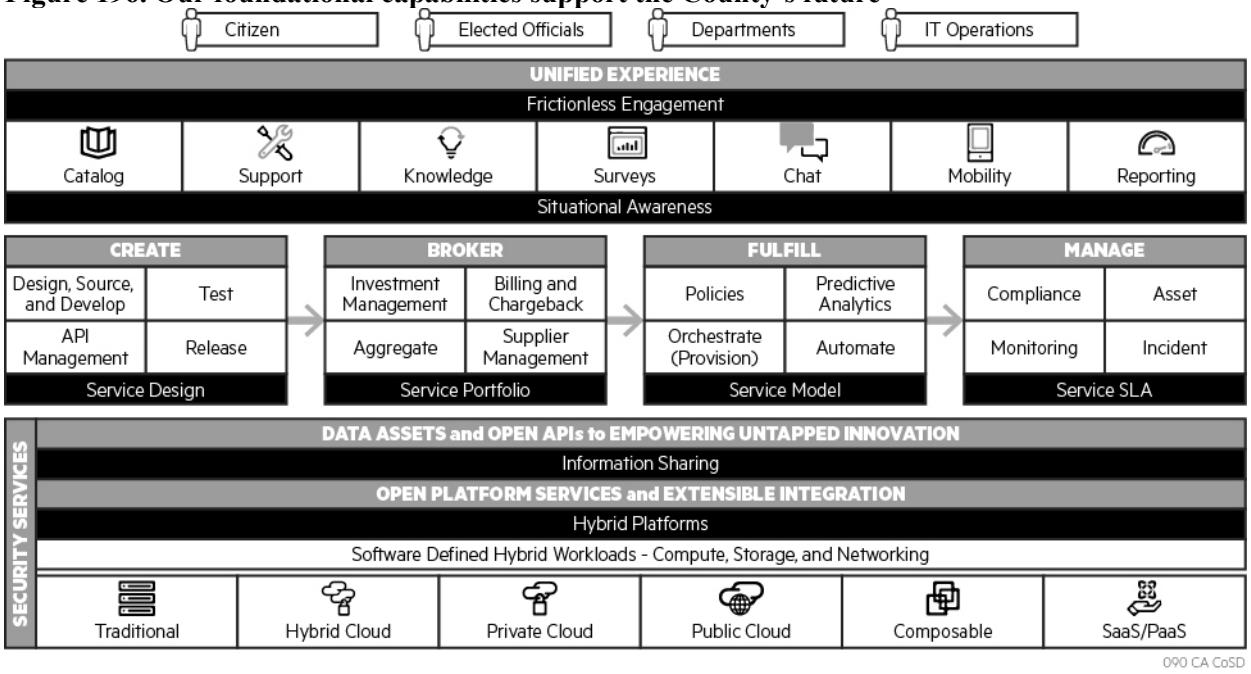
None.

Executive Summary – The County's Future State

As described in our approach to each of the Transformation Projects, HPES will provide the required and recommended transformational mechanisms to generate new ideas, foster a new way thinking (bi-modal), and spark creativity within the employee teams across the County and industry partners—to collectively realize the benefits of transformational activities.

Our implementation of these Transformation Projects will put the County in the position to support the next generation of employees and citizens who are proactive, connected, collaborative, and aspiring to contribute. This future state is depicted in Figure 196. Providing access to open platforms, tools, and data services enables citizens to participate in transformational activities.

Figure 196. Our foundational capabilities support the County's future



As the County continues moving forward, it will deliver more and more services to constituents that are easily accessible and facilitate information sharing and consumption.

Cross-Framework/Component Integration: When identifying and assessing opportunities for transformation, HPES has the experience with the County to understand the complete picture to make sure that Transformation Projects are compatible and that their implementation will flawlessly integrate with the existing environment.

Competitive Differentiators and Benefits to the County: Through our experience under the current contract, HPES is best qualified to identify, assess, and implement Transformational Projects that maximize the reuse of existing technology and return on investment (RoI), while taking into consideration the County's culture and the needs of the businesses and citizens that interact with the County. HPES' recommendations for Transformation Projects will be built on the following:

- **A Thorough Understanding of County Business:** Our experience working side-by-side with the County gives us an advantage in understanding the Operational Plan, priorities, goals, objectives, preferences, and approaches. This is applicable to governance, reporting, County interactions, and delivery of services.
- **Reliability:** The County has a critical mission in providing services to residents, including support of safe communities, sustainable environments, and healthy families. Many of these services rely on IT systems that must be capable of growing and changing to meet County objectives.
- **Predictability:** HPES recognizes the importance of predictability in the annual budgeting process, and we understand that this is a critical element of any Transformation Project. We know the County's budgeting process, and we understand that the County will rely on the cost inputs that we provide. As such, we are diligent in our estimating so that our costs are reliable and predictable and help to avoid budget issues for the County.

- **Innovation/Technology Leadership:** HPES is a cornerstone in the IT industry, and we are at the forefront of technology innovation. We recognize that local government depends on getting the right technologies in place to support the new era of digital government services; HPES can provide those technologies. HPE Labs invests more than $2 billion per year in research and development to bring innovation to our clients. This includes investment to develop one of the broadest portfolios of cloud services in the market. At the local (account) level, we built on the County Innovation initiative and created an Innovation Council to identify and develop new ideas, technologies, and processes to benefit the County. The Innovation Council's intent is to address real business needs and reduce costs as well as to increase efficiency and productivity. The next step in the evolution of the Innovation Council will be to add representation from HPE Labs and forge a sustained relationship between the Chief Technology Officer (CTO), the HPES account, and HPE Labs. To the extent allowed by County HR guidelines, HPES welcomes Innovation Council membership and participation from County Departments and County End-Users.
- **Depth and Breadth:** As a world-class provider of IT services, HPES has the capabilities necessary to help move the County forward through new technology implementation and new processes to speed service delivery to constituents. Along with our key partner AT&T, HPES has proven that we have the depth, breadth, and staff knowledge to continue to transform County services. In addition, HPES is a stable, recognizable, financially strong company that you can rely on to be your trusted partner and provider for years to come.

2.13 Offeror Response to Exhibit O-Schedule 7.6 Shared Resources

Offeror to provide information as instructed in Exhibit O-Schedule 7.6 Shared Resources and provide as an appendix with populated information.

Following is a list of the shared resources used in our solution to provide services to the County. The list consists primarily of software tools. For software or infrastructure that runs in the data center, or as a service, the County should infer that the hardware that runs this software is also a shared resource, with appropriate security boundaries in place to protect County data. In the interest of brevity we have not listed these related hardware components. For software that runs on individual workstations, items included here are licensed by HPES or its partners for use in supporting our customers, but are not specifically licensed for any specific customer.

Version numbers and tools are accurate as of the time of this proposal submission. Note that version numbers on HPE software commercial products customized for HPES internal use may not coincide with the version numbers available to the public.

Table 88. Cross-Functional Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
Enterprise System List (ESL)	Type: Software Manufacturer: HPES Version: 16.1.1 Purpose/Use: ESL (Enterprise System List) is a Delivery-focused Configuration Management System for managing System/Application Configuration Items, Services/Contracts and Customer/Account Information. Other Information:
Asset Manager	Type: Software Manufacturer: HPE Version: 3.7P1 Purpose/Use: Tracks end-user and network assets Other Information:
Discovery and Dependency Mapping Inventory (DDMI)	Type: Software Manufacturer: HPE Version: 9.32 P1 Purpose/Use: discovers and reports assets found on the network; integrates with Asset Manager. Other Information:
Service Manager	Type: Software Manufacturer: HPE Version: 4.0.5p31 Purpose/Use: Used by the Service Desk and all support staff for ticketing of Incidents, Problems and Changes. Other Information:
Request Manager	Type: Software Manufacturer: HPE Version: 2.5.1.R2.22

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: Used to enter and manage Service Requests and Catalog items. Other Information:
End User Access (EUA)	Type: Software Manufacturer: HPES Version: 2.1.6 Purpose/Use: Service Portal Other Information: While the core software and interfaces are standardized and centrally controlled to interact with the rest of the cross functional tools, the Service Portal is separately instantiated and customized for each client for whom it is deployed.
Aries/Aldea	Type: Software Manufacturer: HPES Version: 3.5.6 / 8.9.3 Purpose/Use: Tool used by HPES internally to request resources (e.g., staffing assignments, workload placement) from the broader HPE community Other Information:
RevGen	Type: Software Manufacturer: SAP Ariba Version: 9r1 Purpose/Use: Procurement of products and services Other Information:
Enabling Delivery and Global Excellence (EDGE)	Type: Knowledge Repository Manufacturer: HPES Version: 4.3 Purpose/Use: EDGE is a holistic environment that includes all the information needed to enable Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE supports all individuals in each of the ES business units by providing process artifacts that can be leveraged and used as part of their day-to-day work. Other Information:
Enterprise Architect	Type: Software Manufacturer: Sparx Systems Version: 9.3 Purpose/Use: Enterprise Architect provides full life cycle modeling for: Business and IT systems Software and Systems Engineering Real-time and embedded development Other Information:
ProVision	Type: Software Manufacturer: OpenText Version: 9.0.2

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: ProVision is HPES's standard modeling tool, to be used for Business Process, Enterprise Architecture and IT solution modeling. It enables business & IT teams to visually create models, describing business process, process interactions and detailed workflow Other Information:
Disaster Recovery Subscription Services, consisting of all leveraged hardware and software used to provide: Server services Storage services Network services Security services Backup services	Type: Disaster Recovery Subscription Services Manufacturer: various Version: N/A Purpose/Use: Leveraged hardware and software Other Information: Note that the Centera and the dedicated firewalls located in the DR site are not considered to be part of this list, since they are dedicated to the County.
ArcSight Security Information and Event Management (SIEM)	Type: Software/appliance Manufacturer: HPE Version: 6.9.1 Purpose/Use: Event logging and monitoring Other Information:
Global Delivery Capacity & Performance Management (GDCPM)	Type: Software Manufacturer: HPES (based on SAS and other underlying tools) Version: 2.0 Purpose/Use: Collects, aggregates and analyzes capacity and performance data from various disparate sources for reporting and analysis Other Information:

Service Desk Equipment, Software, Tools, and Systems

Note: Software used in providing Service Desk services is listed in the Cross-Functional section, since this software is also used by other frameworks.

IVR and ACD hardware and software, and other tools/facilities used by the Service Desk are internal to HPE, and are not listed individually

Table 89. End-User Equipment, Software, Tools and Systems

RESOURCE / TOOL NAME	INFORMATION
System Center Configuration Manager (SCCM)	Type: Software Manufacturer: Microsoft Version: 2012 Purpose/Use: Discovery and software distribution to end-user devices Other Information:

Table 90. Network Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
Leveraged Internet Service (LIS) firewalls in the Tulsa and Colorado Springs data centers	Type: Hardware Manufacturer: Checkpoint Version: D2 Purpose/Use: Internet access/security Other Information: In the future these are slated to be replaced by Fortinet firewalls
AT&T Commonly Shared Network	Type: equipment, tools, software, systems and other materials Manufacturer: Various Version: N/A Purpose/Use: For clarity, the AT&T Commonly Shared Network means (i) the public or shared networks of AT&T, its Affiliates and their subcontractors, and the equipment, tools, technologies, systems, software, and other materials that are components thereof; (ii) equipment, tools, technologies, systems, software and other materials used by AT&T, its Affiliates and their subcontractors in shared network management and back office environments including , without limitation, TIRKs, iGEMS, BusinessDirect, Billing Edge, the AT&T Global Network Client and AT&T Connect and any other items listed above in this Exhibit; and (iii) all modifications, upgrades, derivative works, enhancements, improvements and extensions of any of the foregoing.
SIMS (Security Information Management System)	Type: Software Manufacturer: AT&T Version: n/a Purpose/Use: Security event correlation Other Information:
SDNOM (Software Defined Network Order Management)	Type: Software Manufacturer: AT&T Version: 1.0 Release 1604 Purpose/Use: Circuit Ordering Other Information:
Nectar Unified Communication Management Platform	Type: Software Manufacturer: Nectar Version: 5.5.2.1 Purpose/Use: Voice Network Performance Management Other Information:
MDM-Airwatch SaaS Console (Mobile Device Management)	Type: Software Manufacturer: AT&T Version: 8.2 Purpose/Use: Mobile device management Other Information:
SORD (Service Order Retrieval and Distribution)	Type: Software Manufacturer: AT&T Version: 8.1.10

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: Service order entry Other Information:
Telegence	Type: Software Manufacturer: AT&T Version: 1602.3 Purpose/Use: Billing Other Information:
BOSS (Billing and Ordering Support System)	Type: Software Manufacturer: AT&T Version: 8.1.01 Purpose/Use: Product billing, tracking and reporting Other Information:
DPSS (Data Products and Services System)	Type: Software Manufacturer: AT&T Version: N/A Purpose/Use: Data product and services tracking Other Information:
BusinessDirect/eBill	Type: Software Manufacturer: AT&T Version: N/A Purpose/Use: Account management Other Information:
Exchange Plus	Type: Software Manufacturer: AT&T Version: 13.1 Purpose/Use: Carrier resource tracking Other Information:
ICES (Integrated Customer Enterprise System) ServiceCenter/AssetCenter	Type: Software Manufacturer: AT&T Version: 5.1.2 Purpose/Use: Asset Inventory Other Information:
SAINT	Type: Software Manufacturer: AT&T Version: 7.20.13 Purpose/Use: Security scanning and testing Other Information:
Nmap	Type: Software Manufacturer: Nmap Version: v7.0 Purpose/Use: Network scanning and mapping Other Information:
WFA (Work Force Administration)	Type: Software Manufacturer: Telcordia

RESOURCE / TOOL NAME	INFORMATION
	Version: n/a Purpose/Use: Trouble ticketing and work flow Other Information:
TIRKS (Trunks Integrated Record Keeping System)	Type: Software Manufacturer: Telecordia Version: n/a Purpose/Use: Circuit design Other Information:
AOTS-TM (AT&T One Ticketing System – Trouble Management)	Type: Software Manufacturer: AT&T/Remedy Version: n/a Purpose/Use: trouble ticketing Other Information:
NMA (Network Monitoring and Analysis)	Type: Software Manufacturer: Telecordia Version: n/a Purpose/Use: Network monitoring Other Information:
Avaya Site Administration	Type: Software Manufacturer: Avaya Version: 6.0 Purpose/Use: Voice system administration Other Information:

Table 91. Data Center Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
Server Automation	Type: Software Manufacturer: HPE Software Version: 10.11 Purpose/Use: Distributing operating system and layered product patches and upgrades Other Information: The core mesh is a shared resource; distribution satellite servers within the County's network zones are dedicated to the County
Operations Manager	Type: Software Manufacturer: HPE Software Version: 9.2 Purpose/Use: Monitoring and alerting for various data center components, such as servers, domain controllers, databases, etc.
Microsoft Office 365 Government Community Cloud	Type: Software as a Service Manufacturer: Microsoft Version: 2016

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: E-Mail (Exchange Online), Collaboration (SharePoint Online, Skype for Business), Cloud File Management (OneDrive for Business)
E2E Complete	Type: Software Manufacturer: BinaryTree Version: 4.0 Purpose/Use: Automation tool for migration of mail services from Exchange to the Microsoft Office 365 Cloud
Helion Virtual Private Cloud for US Public Sector	Type: Infrastructure as a Service Manufacturer: HPES Version: 7.6 Purpose/Use: Virtual Private Cloud (VPC) for Windows and Linux environments. VPC is a Government Community Cloud currently used to run the County's Beach and Water Quality website.
Watchdog	Type: Software Manufacturer: HPES Version: N/A Purpose/Use: Internally developed utility that monitors/removes privileged access implemented via non-approved methods

Applications Maintenance and Operations Equipment, Software, Tools and Systems

All tools identified for applications development below may also be used in the applications Maintenance and Operations (M&O) environment.

Table 92. Applications Development Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
StarTeam	Type: Software Manufacturer: Microfocus/Borland Version: N/A Purpose/Use: Software Change and Configuration Management Other Information: This tool may also be used in Business Analysis and Applications M&O
Together	Type: Software Manufacturer: Microfocus/Borland Version: N/A Purpose/Use: Together enables software to be designed using industry-standard UML notation and conventions. With a large number of built-in utilities to manage the software design process, validate designs and generate code, Together helps maximize the efficiency and accuracy of the software development process Other Information: This tool may also be used in Business Analysis and Applications M&O
Agile Manager	Type: Software Manufacturer: HPE

RESOURCE / TOOL NAME	INFORMATION
	Version: N/A Purpose/Use: Agile project management is a SaaS (software-as-a-service) solution that helps teams to organize, plan, and execute Agile projects. Other Information: This tool may also be used in Business Analysis and Applications M&O
Team Foundation Server	Type: Software Manufacturer: Microsoft Version: N/A Purpose/Use: Microsoft Team Foundation Server (TFS) is a set of tools and technologies that enable a team to collaborate and coordinate the development and build efforts for a .NET software product or completing a .NET software project. Other Information: This tool may also be used in Business Analysis and Applications M&O

2.14 Offeror Response to Exhibit Q-Schedule 10.1.1 Contractor Key Personnel

Offeror to provide a proposed list of named individuals listed in Exhibit Q-Schedule 10.1.1 Contractor Key Personnel.

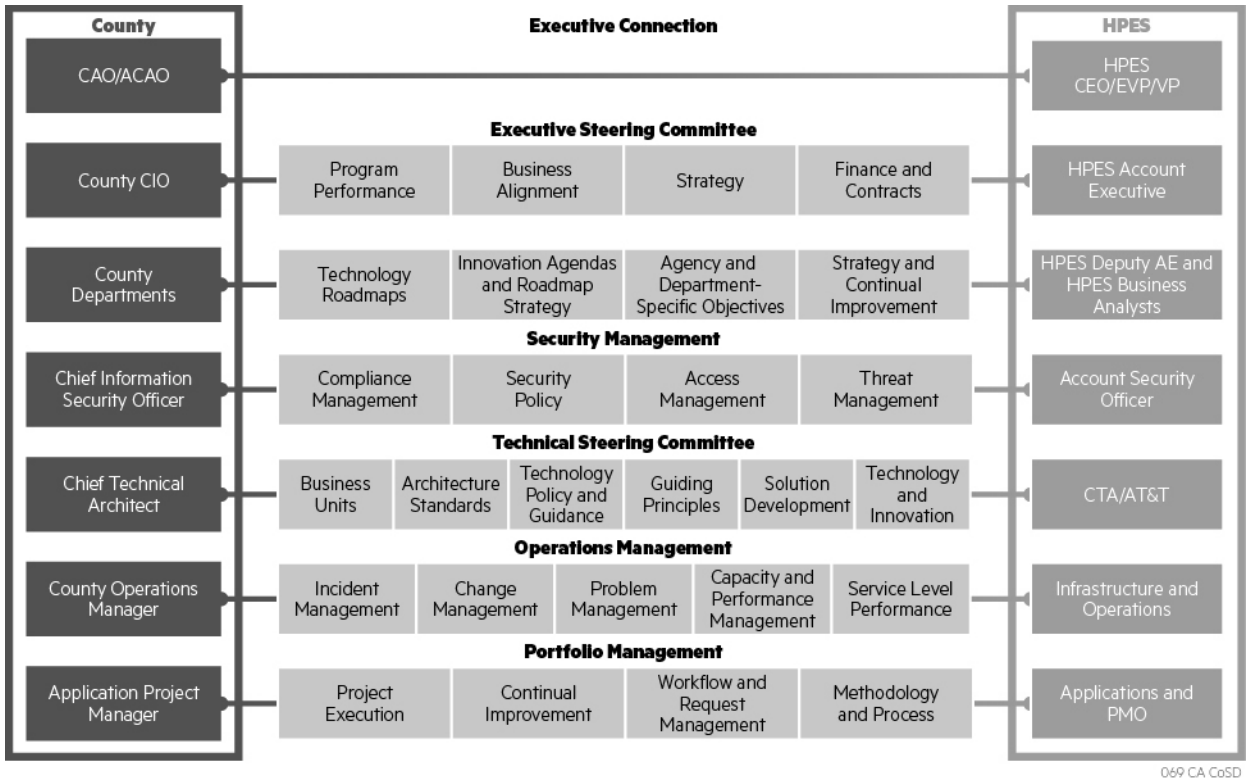
KEY POSITIONS	PROPOSED NAMED INDIVIDUAL
Account Executive	Cathy Varner
Deputy Account Executive	Laura Floyd
Enterprise Service Delivery Manager (SDM)	Kathleen Barghols
FG3 Service Delivery Manager (SDM)	John Steed
CSG Service Delivery Manager (SDM)	Frank Krone
HHSA Service Delivery Manager (SDM)	Sandra Messina
PSG Service Delivery Manager (SDM)	Albert Hatcher
LUEG Service Delivery Manager (SDM)	David Pugh
Contracts Manager	Max Pinna
Chief Information Security Officer (CISO)	Marcelo Peredo
Chief Technology Architect (CTA)	Thif Iruthayarajah
Cross Functional Services Manager	Mark Morin
Service Desk Manager	Curtis Yancey
End User Services Manager	Hector Vaquedano
Network Services Manager	Jeff Williams
Data Center Services Manager	Michael Boscarino
Application Maintenance and Operations Services Manager	Tina Terlecki
Applications Development Services Manager	Mark Roehr
Project Management Office (PMO) Manager	Nelson Diaz
Transition Services Manager	Chris Spanka

2.15 Offeror Response to Exhibit R-Schedule 10.3 Relationship Management

Offeror to propose a counterpart for relationship management between the County on the Offeror organization.

HPES has implemented a multi-tiered relationship framework for communication and decision- making that provides effective collaboration and timely action. This framework, illustrated in Figure 197, maximizes communication based on the County's organizational structure. HPES and County leaders are aligned to the framework to produce results consistent with technical and process architectures. From requirements definition to solution realization, this framework fosters an in depth understanding of business needs and effectively identifies opportunities for innovation and process improvement to the benefit of the County. The framework supports the collaborative development of plans of action based on agreed decisions to achieve the best outcomes for County staff and its citizens. HPES will work with the County to facilitate alignment to the existing governance within the County Technology Office (CTO) and individual County groups.

Figure 197. Multi-tiered Interactive Framework for Communication



HPES' relationship framework aligns HPES and County leaders to foster clear communication, a solid understanding of business needs, and opportunities for innovation and improvement.

We designed the HPES-County of San Diego Account organization structure to achieve the best balance of economy and effectiveness. Senior staff are assigned to lead each functional area for this program. The HPES account team is made up of highly qualified experts—with more than 320 years of combined experience supporting the County. This multitiered relationship framework builds mutual trust and results in effective, collaborative interactions with everyone focused on getting from idea to value as quickly and efficiently as possible.

2.15.1 Relationship Counterpart

Table 93 outlines the relationship counterparts between the County and HPES roles.

Table 93. Relationship Counterpart

COUNTY OF SAN DIEGO	HPES
CIO	Vice President and Account Executive (AE)
ACIO	Deputy AE
GITMs	Deputy AE, Enterprise Service Delivery Manager, Service Delivery Managers, Applications Development Services Manager, Project Management Office Manager
CTA	CTA
Contracts Manager	Contracts Manager
Chief Information Security Officer	Chief Information Security Officer
Applications Management	Applications development services manager
Chief Data Architect	CTA
Enterprise Application Project Manager	Project Management Office Manager
Operations Managers	Service Delivery Managers

To enhance this multitiered framework, a complementing communication matrix has been established based on the County's organizational structure and requirements that substantiate the County and HPES leadership and operational teams are focused and informed on the needs of the County. Table 94 outlines the proposed stakeholder communication matrix to facilitate a strong communication and collaboration to advance County business and technical objectives.

Table 94. Proposed Stakeholder Communication Matrix

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
Executive Meeting	HPES/County Alignment of Objectives and Program Escalations	Bimonthly, or as determined by the County participant	County CIO, HPES State and Local Government VP and HPES AE
Program Status and Strategy	Program management overall program health	Weekly	County CIO, HPES AE
CIO Security Briefing	Briefing to County CIO on security strategy, initiatives, and status	Monthly	County CISO. HPES CISO and HPES security officer
Executive Liaison Program Meetings	One-on-one communication between HPES AE and key County stakeholders to discuss vision and strategy. Intent is to make certain HPES is prepared to respond to County requirements.	Quarterly, biannually, or annually, as determined by the County participant	County GMs, ROV, DHR, County Council, and select elected officials, HPES AE and/or deputy AE

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
CTO Enterprise Architecture Meetings	Review enterprise architecture solution designs, annual updates to hardware and software standards for servers, and end-user compute devices, exceptions to standards via notice of decisions, vendor technology roadmaps	Weekly	County CTA, CTO IT Staff, GITMs, County agency and/or department representation, HPES CTA, HPES technology office and other HPES leaders, as needed.
Enterprise Architecture Review	Reviews proposed architectural changes, large project designs, architectural issues	Weekly	County CTA, CTO IT staff, GITMs. HPES CTA, HPES technology office, and other HPES leaders, as needed.
Network Architecture Meetings	Review network roadmaps and technology upgrades	Weekly	County CTA and other CTO IT staff. HPES CTA, and other HPES technical leaders, as needed, AT&T chief architect
Core Meeting	Preview enterprise solution designs (detailed walkthrough) and changes to standards	Weekly	County CTA, CTO IT staff and CISO. HPES CTA, HPES CISO, and other HPES leaders, as needed
Infrastructure Project Review	Provides schedule, issue, and status data for active infrastructure projects	Weekly	County CTA, GITMs, CTO IT staff. HPES CTA, HPES technology office, and other HPES leaders, as needed
Platform Status Reviews	Review project for critical County application platforms	Weekly	County CTA, CTO IT staff. HPES Application Development Leader and other HPES Leaders, as needed.
Portfolio Review	Provide review of high visibility, critical projects	Monthly	County CTA, GITMs, and CTO IT Staff. HPES business analysts, HPES deputy AE and other HPES leaders, as needed
Portfolio Steering Committees	Review portfolio and future plans	Quarterly	County GITMs. HPES Business Analysts, and other HPES leaders, as needed
ITPMO Review	Discuss processes and procedures related to project	Weekly	County CTO IT staff, CTA, HPES PMO and

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
	management and process improvement with CTO		other HPES leaders, as needed
Quarterly Program Review	Provide program status, accomplishments, and operational data	Quarterly	County CTO IT staff, CTA and GITMs. HPES AE, Deputy AE, and other HPES leaders, as needed *
Service Delivery Operations	Mitigation/review of operation changes and issues with CTO	Biweekly	County CTO IT staff, CTA. HPES Service Delivery Executive, and other HPES leaders, as needed
Service Delivery Operations Monthly	Mitigation/review of operation changes and issues with the County Technology Office (CTO) and GITMs	Monthly	County CTA, CTO IT staff, and GITMs. HPES service delivery executive, SDMs, and other HPES leaders, as needed
County Bricks (Technology Standards)	Document past, current, and future technology standards using Gartner's Brick framework. Bricks guides solutions for the County and is updated when there are specific changes to a technology item.	As needed, triggered by product, vendor, or technology changes	County CTO IT staff, CTA, GITMs. HPES CTA, HPES technology office and other HPES leaders, as needed *
Voice of the Client (VOC) – Service Excellence Initiative	Includes self-assessed ratings pertaining to delivery and client satisfaction results based on client survey feedback; our objective is continual improvement of client satisfaction and retention	Yearly	County CTO IT staff. HPES VOC Interviewer
Information Technology Improvement Needs Assessment (ITINA) Process	HPES provides support for the County enterprise IT project planning and budgeting process—prioritization, estimating, and selection for County enterprise IT initiatives	Yearly	County IT Planning Board, GITMs, CTO IT staff, HPES participants based on subject matter expertise

**HPES Technology Team includes AT&T*

2.16 Offeror Response to Exhibit Y: Schedule 14.1 Approved Subcontractors

Offeror to complete the table in Exhibit Y-Schedule 14.1 Approved Subcontractors and provide as an appendix.

Table 95. Key Subcontractors of Contractors

NAME	DATE ADDED TO SCHEDULE
AT&T Corp.	To be added at contract award.

2.17 Assumptions

Assumptions for the technical response made by the Offeror in responding to this RFP do not obligate the County in any way. The number and extent of assumptions made by the Offeror may impact the score in the evaluation. Additionally, assumptions made by the Offeror may make the Proposal conditional and may cause the Offeror's Proposal to be rejected.

None.

2.18 Offeror Response to Technical Exception List

Schedule 4.3 Operational Services has been provided in PDF format as part of the RFP (see Exhibit H-Schedule 4.3 Operational Services).

The Contractor shall provide a response to Exhibit H-Schedule 4.3 Operational Services in the following format:

Table 100: Exception List

ITEM #	Technical REFERENCE (Schedule/Exhibit, Section, Page, Paragraph)	Exception (Short Description of text or requirement)	OFFEROR PROPOSED SOLUTION/RATIONALE AND BENEFITS OF PROPOSED SOLUTION TO THE COUNTY	N (Not Met) R (Revised Approach)
1.	Exhibit J, Schedule 4.8 Service Levels, 7.6 First Call Resolution (SL 28)	We propose that the County accept the performance target of 70% with < 5% recalls offered in our solution.	Seventy percent (70%) first-call resolution rate (FCR) is the industry-accepted service level. Gartner reports, under Service Desk Statistics on FCR, 2014, the industry average has dropped to 63%. Indeed, HPES' review of Service Desk statistics in general found that once self-service is introduced, FCR falls because the overall ticket volume decreases resulting in an increase in the proportion of tickets requiring SME support.	R
2.	Exhibit J, Schedule 4.8 Service Levels, Section 4.8, SL 10.2 Daily Backup (SL40)	We propose that the County accept the performance target of 99% offered in our solution.	98% is standard in the industry. 99% is the SL we are subject to today. We believe that the additional cost to provide the additional .9% may not justify the benefit. We invite further discussion on this topic if the County strongly requires 99.9% performance.	R
3.	Exhibit J, Schedule 4.8 Service Levels, Section 4.8, SL 11.4 Application Availability (SL51)	HPES is being held accountable for environments where the configurations are not within our control.	We accept the Service Level requirement, but propose excluding the following scenarios: Application environments that have performance issues not within HPES' control to correct	R
4.	Exhibit J, Schedule 4.8 Service Levels, 11.6 Application Respond Time (SL 53)	HPES is being held accountable for environments where the configurations are not within our control. The list of Applications and Transactions subject to this	We accept the Service Level requirement, but propose excluding the following scenarios: Application environments that have performance issues not within HPES' control to correct We propose defining a specific list of Applications and Transactions subject to this Service Level so that its measurement can be instrumented without putting undue strain on the network and potentially requiring an infrastructure cost	R

ITEM #	Technical REFERENCE (Schedule/Exhibit, Section, Page, Paragraph)	Exception (Short Description of text or requirement)	OFFEROR PROPOSED SOLUTION/RATIONALE AND BENEFITS OF PROPOSED SOLUTION TO THE COUNTY	N (Not Met) R (Revised Approach)
		service level is not defined. Low performance network is not defined.	that outweighs the value of the Service Level to the County. Defining the term will prevent future disputes.	

2.19 Appendix - Completed Exhibits

Exhibit O: Schedule 7.6 Shared Resources

Offeror to provide information as instructed in Exhibit O-Schedule 7.6 Shared Resources and provide as an appendix with populated information.

Following is a list of the shared resources used in our solution to provide services to the County. The list consists primarily of software tools. For software or infrastructure that runs in the data center, or as a service, the County should infer that the hardware that runs this software is also a shared resource, with appropriate security boundaries in place to protect County data. In the interest of brevity we have not listed these related hardware components. For software that runs on individual workstations, items included here are licensed by HPES or its partners for use in supporting our customers, but are not specifically licensed for any specific customer.

Version numbers and tools are accurate as of the time of this proposal submission. Note that version numbers on HPE software commercial products customized for HPES internal use may not coincide with the version numbers available to the public.

Table 96. Cross-Functional Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
Enterprise System List (ESL)	Type: Software Manufacturer: HPES Version: 16.1.1 Purpose/Use: ESL (Enterprise System List) is a Delivery-focused Configuration Management System for managing System/Application Configuration Items, Services/Contracts and Customer/Account Information. Other Information:
Asset Manager	Type: Software Manufacturer: HPE Version: 3.7P1 Purpose/Use: Tracks end-user and network assets Other Information:
Discovery and Dependency Mapping Inventory (DDMI)	Type: Software Manufacturer: HPE Version: 9.32 P1 Purpose/Use: discovers and reports assets found on the network; integrates with Asset Manager. Other Information:
Service Manager	Type: Software Manufacturer: HPE Version: 4.0.5p31 Purpose/Use: Used by the Service Desk and all support staff for ticketing of Incidents, Problems and Changes. Other Information:
End User Access (EUA)	Type: Software Manufacturer: HPES Version: 2.1.6 Purpose/Use: Service Portal

RESOURCE / TOOL NAME	INFORMATION
	Other Information: While the core software and interfaces are standardized and centrally controlled to interact with the rest of the cross functional tools, the Service Portal is separately instantiated and customized for each client for whom it is deployed.
Aries/Aldea	Type: Software Manufacturer: HPES Version: 3.5.6 / 8.9.3 Purpose/Use: Tool used by HPES internally to request resources (e.g., staffing assignments, workload placement) from the broader HPE community Other Information:
RevGen	Type: Software Manufacturer: SAP Ariba Version: 9r1 Purpose/Use: Procurement of products and services Other Information:
Enabling Delivery and Global Excellence (EDGE)	Type: Knowledge Repository Manufacturer: HPES Version: 4.3 Purpose/Use: EDGE is a holistic environment that includes all the information needed to enable Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE supports all individuals in each of the ES business units by providing process artifacts that can be leveraged and used as part of their day-to-day work. Other Information:
Enterprise Maps	Type: Software Manufacturer: HPE Version: 3.0 Purpose/Use: HPE Enterprise Maps software plans and drives IT transformation roadmaps by mapping the overall IT landscape with business outcomes. Other Information: Enterprise Maps is certified as ArchiMate 2 Tool and incorporates principles from TOGAF Enterprise Architecture Framework
Enterprise Architect	Type: Software Manufacturer: Sparx Systems Version: 9.3 Purpose/Use: Enterprise Architect provides full life cycle modeling for: Business and IT systems Software and Systems Engineering Real-time and embedded development Other Information:
ProVision	Type: Software Manufacturer: OpenText

RESOURCE / TOOL NAME	INFORMATION
	Version: 9.0.2 Purpose/Use: ProVision is HPES's standard modeling tool, to be used for Business Process, Enterprise Architecture and IT solution modeling. It enables business & IT teams to visually create models, describing business process, process interactions and detailed workflow Other Information:
Disaster Recovery Subscription Services, consisting of all leveraged hardware and software used to provide: Server services Storage services Network services Security services Backup services	Type: Disaster Recovery Subscription Services Manufacturer: various Version: N/A Purpose/Use: Leveraged hardware and software Other Information: Note that the Centera and the dedicated firewalls located in the DR site are not considered to be part of this list, since they are dedicated to the County.
ArcSight Security Information and Event Management (SIEM)	Type: Software/appliance Manufacturer: HPE Version: 6.9.1 Purpose/Use: Event logging and monitoring Other Information:
Global Delivery Capacity & Performance Management (GDCPM)	Type: Software Manufacturer: HPES (based on SAS and other underlying tools) Version: 2.0 Purpose/Use: Collects, aggregates and analyzes capacity and performance data from various disparate sources for reporting and analysis Other Information:

Service Desk Equipment, Software, Tools, and Systems

Note: Software used in providing Service Desk services is listed in the Cross-Functional section, since this software is also used by other frameworks.

IVR and ACD hardware and software, and other tools/facilities used by the Service Desk are internal to HPE, and are not listed individually

Table 97. End-User Equipment, Software, Tools and Systems

RESOURCE / TOOL NAME	INFORMATION
System Center Configuration Manager (SCCM)	Type: Software Manufacturer: Microsoft Version: 2012 Purpose/Use: Discovery and software distribution to end-user devices Other Information:

Table 98. Network Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
Leveraged Internet Service (LIS) firewalls in the Tulsa and Colorado Springs data centers	Type: Hardware Manufacturer: Checkpoint Version: D2 Purpose/Use: Internet access/security Other Information: In the future these are slated to be replaced by Fortinet firewalls
AT&T Commonly Shared Network	Type: equipment, tools, software, systems and other materials Manufacturer: Various Version: N/A Purpose/Use: For clarity, the AT&T Commonly Shared Network means (i) the public or shared networks of AT&T, its Affiliates and their subcontractors, and the equipment, tools, technologies, systems, software, and other materials that are components thereof; (ii) equipment, tools, technologies, systems, software and other materials used by AT&T, its Affiliates and their subcontractors in shared network management and back office environments including , without limitation, TIRKs, iGEMS, BusinessDirect, Billing Edge, the AT&T Global Network Client and AT&T Connect and any other items listed above in this Exhibit; and (iii) all modifications, upgrades, derivative works, enhancements, improvements and extensions of any of the foregoing.
SIMS (Security Information Management System)	Type: Software Manufacturer: AT&T Version: n/a Purpose/Use: Security event correlation Other Information:
SDNOM (Software Defined Network Order Management)	Type: Software Manufacturer: AT&T Version: 1.0 Release 1604 Purpose/Use: Circuit Ordering Other Information:
Nectar Unified Communication Management Platform	Type: Software Manufacturer: Nectar Version: 5.5.2.1 Purpose/Use: Voice Network Performance Management Other Information:
MDM-Airwatch SaaS Console (Mobile Device Management)	Type: Software Manufacturer: AT&T Version: 8.2 Purpose/Use: Mobile device management Other Information:
SORD (Service Order Retrieval and Distribution)	Type: Software Manufacturer: AT&T Version: 8.1.10

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: Service order entry Other Information:
Telegence	Type: Software Manufacturer: AT&T Version: 1602.3 Purpose/Use: Billing Other Information:
BOSS (Billing and Ordering Support System)	Type: Software Manufacturer: AT&T Version: 8.1.01 Purpose/Use: Product billing, tracking and reporting Other Information:
DPSS (Data Products and Services System)	Type: Software Manufacturer: AT&T Version: N/A Purpose/Use: Data product and services tracking Other Information:
BusinessDirect/eBill	Type: Software Manufacturer: AT&T Version: N/A Purpose/Use: Account management Other Information:
Exchange Plus	Type: Software Manufacturer: AT&T Version: 13.1 Purpose/Use: Carrier resource tracking Other Information:
ICES (Integrated Customer Enterprise System) ServiceCenter/AssetCenter	Type: Software Manufacturer: AT&T Version: 5.1.2 Purpose/Use: Asset Inventory Other Information:
SAINT	Type: Software Manufacturer: AT&T Version: 7.20.13 Purpose/Use: Security scanning and testing Other Information:
Nmap	Type: Software Manufacturer: Nmap Version: v7.0 Purpose/Use: Network scanning and mapping Other Information:
WFA (Work Force Administration)	Type: Software Manufacturer: Telcordia

RESOURCE / TOOL NAME	INFORMATION
	Version: n/a Purpose/Use: Trouble ticketing and work flow Other Information:
TIRKS (Trunks Integrated Record Keeping System)	Type: Software Manufacturer: Telecordia Version: n/a Purpose/Use: Circuit design Other Information:
AOTS-TM (AT&T One Ticketing System – Trouble Management)	Type: Software Manufacturer: AT&T/Remedy Version: n/a Purpose/Use: trouble ticketing Other Information:
NMA (Network Monitoring and Analysis)	Type: Software Manufacturer: Telecordia Version: n/a Purpose/Use: Network monitoring Other Information:
Avaya Site Administration	Type: Software Manufacturer: Avaya Version: 6.0 Purpose/Use: Voice system administration Other Information:

Table 99. Data Center Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
Server Automation	Type: Software Manufacturer: HPE Software Version: 10.11 Purpose/Use: Distributing operating system and layered product patches and upgrades Other Information: The core mesh is a shared resource; distribution satellite servers within the County's network zones are dedicated to the County
Operations Manager	Type: Software Manufacturer: HPE Software Version: 9.2 Purpose/Use: Monitoring and alerting for various data center components, such as servers, domain controllers, databases, etc.
Microsoft Office 365 Government Community Cloud	Type: Software as a Service Manufacturer: Microsoft Version: 2016

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: E-Mail (Exchange Online), Collaboration (SharePoint Online, Skype for Business), Cloud File Management (OneDrive for Business)
E2E Complete	Type: Software Manufacturer: BinaryTree Version: 4.0 Purpose/Use: Automation tool for migration of mail services from Exchange to the Microsoft Office 365 Cloud
Helion Virtual Private Cloud for US Public Sector	Type: Infrastructure as a Service Manufacturer: HPES Version: 7.6 Purpose/Use: Virtual Private Cloud (VPC) for Windows and Linux environments. VPC is a Government Community Cloud currently used to run the County's Beach and Water Quality website.
Watchdog	Type: Software Manufacturer: HPES Version: N/A Purpose/Use: Internally developed utility that monitors/removes privileged access implemented via non-approved methods

Applications Maintenance and Operations Equipment, Software, Tools and Systems

All tools identified for applications development may also be used in the applications Maintenance and Operations (M&O) environment.

Table 100. Applications Development Equipment, Software, Tools, and Systems

RESOURCE / TOOL NAME	INFORMATION
StarTeam	Type: Software Manufacturer: Microfocus/Borland Version: N/A Purpose/Use: Software Change and Configuration Management Other Information: This tool may also be used in Business Analysis and Applications M&O
Together	Type: Software Manufacturer: Microfocus/Borland Version: N/A Purpose/Use: Together enables software to be designed using industry-standard UML notation and conventions. With a large number of built-in utilities to manage the software design process, validate designs and generate code, Together helps maximize the efficiency and accuracy of the software development process Other Information: This tool may also be used in Business Analysis and Applications M&O
Agile Manager	Type: Software Manufacturer: HPE

RESOURCE / TOOL NAME	INFORMATION
	Version: N/A Purpose/Use: Agile project management is a SaaS (software-as-a-service) solution that helps teams to organize, plan, and execute Agile projects. Other Information: This tool may also be used in Business Analysis and Applications M&O
Team Foundation Server	Type: Software Manufacturer: Microsoft Version: N/A Purpose/Use: Microsoft Team Foundation Server (TFS) is a set of tools and technologies that enable a team to collaborate and coordinate the development and build efforts for a .NET software product or completing a .NET software project. Other Information: This tool may also be used in Business Analysis and Applications M&O

Exhibit Q: Schedule 10.1.1 Contractor Key Personnel

Offeror to provide a proposed list of named individuals listed in Exhibit Q-Schedule 10.1.1 Contractor Key Personnel.

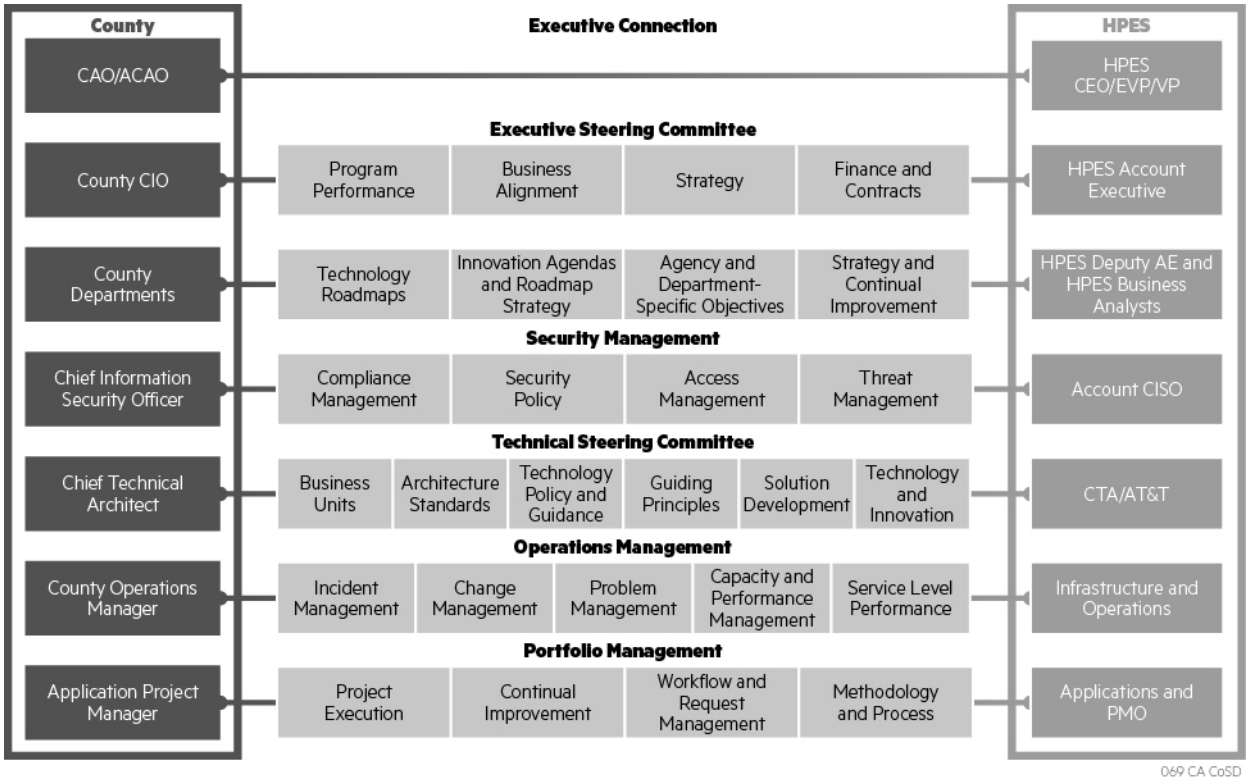
KEY POSITIONS	PROPOSED NAMED INDIVIDUAL
Account Executive	Cathy Varner
Deputy Account Executive	Laura Floyd
Enterprise Service Delivery Manager (SDM)	Kathleen Barghols
FG3 Service Delivery Manager (SDM)	John Steed
CSG Service Delivery Manager (SDM)	Frank Krone
HHSA Service Delivery Manager (SDM)	Sandra Messina
PSG Service Delivery Manager (SDM)	Albert Hatcher
LUEG Service Delivery Manager (SDM)	David Pugh
Contracts Manager	Max Pinna
Chief Information Security Officer (CISO)	Marcelo Peredo
Chief Technology Architect (CTA)	Thif Iruthayarajah
Cross Functional Services Manager	Mark Morin
Service Desk Manager	Curtis Yancey
End User Services Manager	Hector Vaquedano
Network Services Manager	Jeff Williams
Data Center Services Manager	Michael Boscarino
Application Maintenance and Operations Services Manager	Tina Terlecki
Applications Development Services Manager	Mark Roehr
Project Management Office (PMO) Manager	Nelson Diaz
Transition Services Manager	Chris Spanka

Exhibit R: Schedule 10.3 Relationship Management

Offeror to propose a counterpart for relationship management between the County on the Offeror organization.

HPES has implemented a multi-tiered relationship framework for communication and decision- making that provides effective collaboration and timely action. This framework, illustrated in Figure 198, maximizes communication based on the County's organizational structure. HPES and County leaders are aligned to the framework to produce results consistent with technical and process architectures. From requirements definition to solution realization, this framework fosters an in depth understanding of business needs and effectively identifies opportunities for innovation and process improvement to the benefit of the County. The framework supports the collaborative development of plans of action based on agreed decisions to achieve the best outcomes for County staff and its citizens. HPES will work with the County to facilitate alignment to the existing governance within the County Technology Office (CTO) and individual County groups.

Figure 198. Multi-tiered Interactive Framework for Communication



HPES' relationship framework aligns HPES and County leaders to foster clear communication, a solid understanding of business needs, and opportunities for innovation and improvement.

We designed the HPES-County of San Diego Account organization structure to achieve the best balance of economy and effectiveness. Senior staff are assigned to lead each functional area for this program. The HPES account team is made up of highly qualified experts—with more than 320 years of combined experience supporting the County. This multitiered relationship framework builds mutual trust and results in effective, collaborative interactions with everyone focused on getting from idea to value as quickly and efficiently as possible.

Relationship Counterpart

Table 101 outlines the relationship counterparts between the County and HPES roles.

Table 101. Relationship Counterpart

COUNTY OF SAN DIEGO	HPES
CIO	Vice President and Account Executive (AE)
ACIO	Deputy AE
GITMs	Deputy AE, Enterprise Service Delivery Manager, Service Delivery Managers, Applications Development Services Manager, Project Management Office Manager
CTA	CTA
Contracts Manager	Contracts Manager
Chief Information Security Officer	Chief Information Security Officer
Applications Management	Applications development services manager
Chief Data Architect	CTA
Enterprise Application Project Manager	Project Management Office Manager
Operations Managers	Service Delivery Managers

To enhance this multitiered framework, a complementary communication matrix has been established based on the County's organizational structure and requirements that substantiate the County and HPES leadership and operational teams are focused and informed on the needs of the County. Table 102 outlines the proposed stakeholder communication matrix to facilitate a strong communication and collaboration to advance County business and technical objectives.

Table 102. Proposed Stakeholder Communications

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
Executive Meeting	HPES/County Alignment of Objectives and Program Escalations	Bimonthly, or as determined by the County participant	County CIO, HPES State and Local Government VP and HPES AE
Program Status and Strategy	Program management overall program health	Weekly	County CIO, HPES AE
CIO Security Briefing	Briefing to County CIO on security strategy, initiatives, and status	Monthly	County CISO. HPES CISO and HPES security officer
Executive Liaison Program Meetings	One-on-one communication between HPES AE and key County stakeholders to discuss vision and strategy. Intent is to make certain HPES is	Quarterly, biannually, or annually, as determined by the County participant	County GMs, ROV, DHR, County Council, and select elected officials, HPES AE and/or deputy AE

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
	prepared to respond to County requirements.		
CTO Enterprise Architecture Meetings	Review enterprise architecture solution designs, annual updates to hardware and software standards for servers, and end-user compute devices, exceptions to standards via notice of decisions, vendor technology roadmaps	Weekly	County CTA, CTO IT Staff, GITMs, County agency and/or department representation, HPES CTA, HPES technology office and other HPES leaders, as needed.
Enterprise Architecture Review	Reviews proposed architectural changes, large project designs, architectural issues	Weekly	County CTA, CTO IT staff, GITMs. HPES CTA, HPES technology office, and other HPES leaders, as needed.
Network Architecture Meetings	Review network roadmaps and technology upgrades	Weekly	County CTA and other CTO IT staff. HPES CTA, and other HPES technical leaders, as needed, AT&T chief architect
Core Meeting	Preview enterprise solution designs (detailed walkthrough) and changes to standards	Weekly	County CTA, CTO IT staff and CISO. HPES CTA, HPES CISO, and other HPES leaders, as needed
Infrastructure Project Review	Provides schedule, issue, and status data for active infrastructure projects	Weekly	County CTA, GITMs, CTO IT staff. HPES CTA, HPES technology office, and other HPES leaders, as needed
Platform Status Reviews	Review project for critical County application platforms	Weekly	County CTA, CTO IT staff. HPES Application Development Leader and other HPES Leaders, as needed.
Portfolio Review	Provide review of high visibility, critical projects	Monthly	County CTA, GITMs, and CTO IT Staff. HPES business analysts, HPES deputy AE and other HPES leaders, as needed
Portfolio Steering Committees	Review portfolio and future plans	Quarterly	County GITMs. HPES Business Analysts, and other HPES leaders, as needed
ITPMO Review	Discuss processes and procedures related to project management and process improvement with CTO	Weekly	County CTO IT staff, CTA, HPES PMO and other HPES leaders, as needed

COMMUNICATION	PURPOSE/OBJECTIVE	FREQUENCY	AUDIENCE
Quarterly Program Review	Provide program status, accomplishments, and operational data	Quarterly	County CTO IT staff, CTA and GITMs. HPES AE, Deputy AE, and other HPES leaders, as needed *
Service Delivery Operations	Mitigation/review of operation changes and issues with CTO	Biweekly	County CTO IT staff, CTA. HPES Service Delivery Executive, and other HPES leaders, as needed
Service Delivery Operations Monthly	Mitigation/review of operation changes and issues with the County Technology Office (CTO) and GITMs	Monthly	County CTA, CTO IT staff, and GITMs. HPES service delivery executive, SDMs, and other HPES leaders, as needed
County Bricks (Technology Standards)	Document past, current, and future technology standards using Gartner's Brick framework. Bricks guides solutions for the County and is updated when there are specific changes to a technology item.	As needed, triggered by product, vendor, or technology changes	County CTO IT staff, CTA, GITMs. HPES CTA, HPES technology office and other HPES leaders, as needed *
Voice of the Client (VOC) – Service Excellence Initiative	Includes self-assessed ratings pertaining to delivery and client satisfaction results based on client survey feedback; our objective is continual improvement of client satisfaction and retention	Yearly	County CTO IT staff. HPES VOC Interviewer
Information Technology Improvement Needs Assessment (ITINA) Process	HPES provides support for the County enterprise IT project planning and budgeting process—prioritization, estimating, and selection for County enterprise IT initiatives	Yearly	County IT Planning Board, GITMs, CTO IT staff, HPES participants based on subject matter expertise

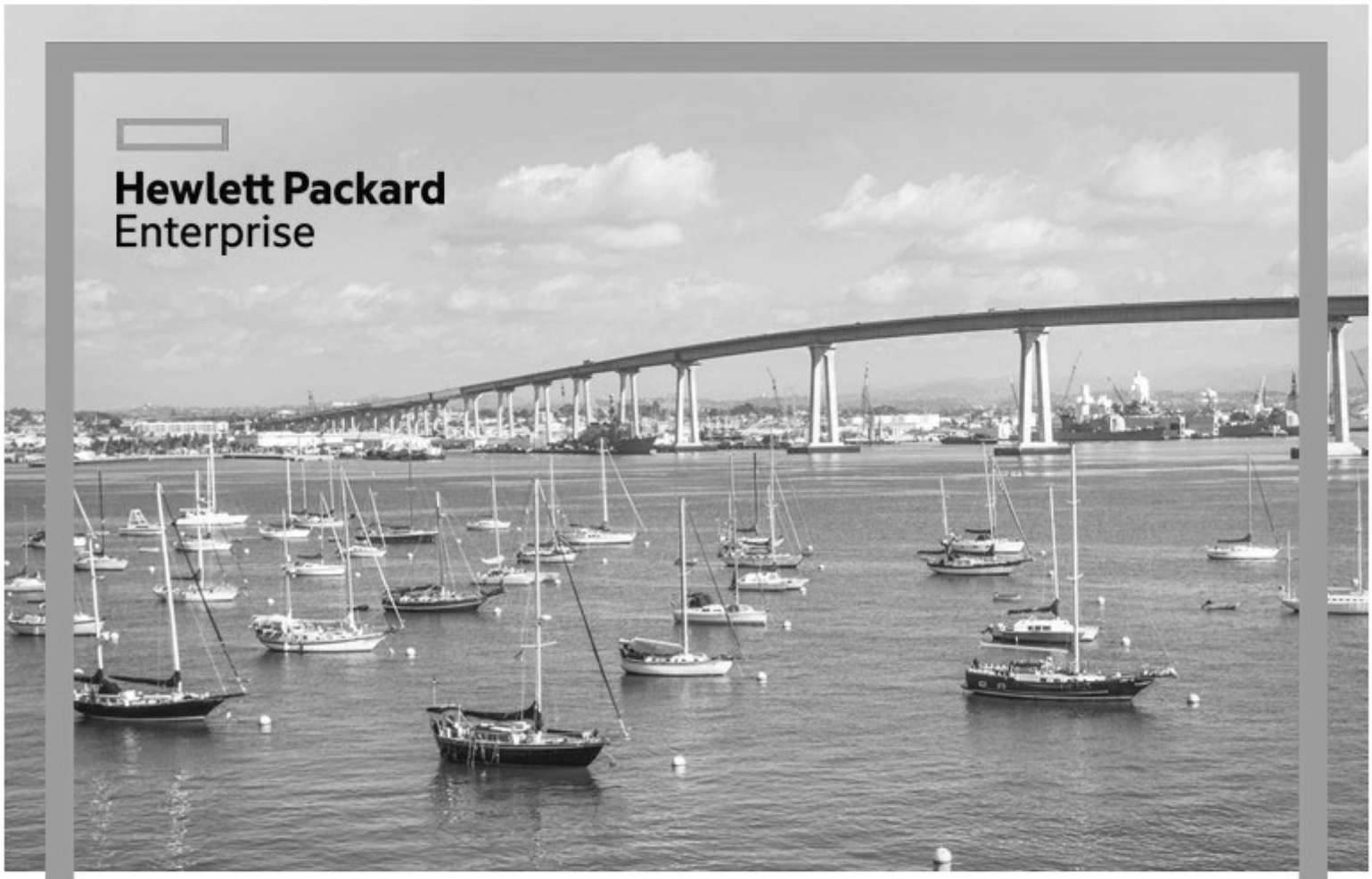
**HPES Technology Team includes AT&T*

Exhibit Y: Schedule 14.1 Approved Subcontractors

Offeror to complete the table in Exhibit Y-Schedule 14.1 Approved Subcontractors and provide as an appendix.

Table 103. Key Subcontractors of Contractors

NAME	DATE ADDED TO SCHEDULE
AT&T Corp.	To be added at contract award.



Hewlett Packard
Enterprise

Driving Results

Committed, progressive partner moving the County forward through innovation and continuous improvement

HP Enterprise Services' Response to the County of San Diego Request for Proposals (RFP) 7189 – Information Technology & Telecommunications Services

Final Submission

October 2016

Volume III - Pricing Proposal

Executive Summary

In recent years, the County of San Diego has transformed the way residents and visitors receive valuable services, obtain information and interact with County officials. With successful efforts to provide digital government, mobility services, business continuity and workforce optimization, the County has been recognized as one of the nation's most technologically advanced counties, achieving numerous awards and accolades. Whereas recognition is notable, the beneficial impact to County employees, taxpayers and residents is what is truly impressive. HPES is proud to have been your partner over the past 10 years in this drive to achieve operational excellence.

HPES understands the County's mission to improve the lives of San Diegans through Safe Communities, Sustainable Environments, Healthy Families, and Operational Excellence. The technology foundation enabling the support of these initiatives relies on systems and services delivered and maintained by our team. Our approach and performance provides the County peace of mind that IT is being managed properly so you can focus on that noblest of motives, the public good.

We must also continue to address the challenges facing County residents, particularly those in danger of being disenfranchised, Veterans, foster children, the homeless, and those suffering from mental illness. We view our role in the County, not just in the context of technology, but as a key enabler to better business outcomes as you strive to "connect the unconnected."

San Diego County has a proud military heritage. Our team will implement programs to support military residents and returning Veterans. Working with groups such as Mission Edge San Diego (Three Wise Men), we will develop training programs tailored for military personnel with the goal of providing the technology skills required to be competitive in the job market.

The County has been successful in raising the "IT IQ" of County personnel. We embrace this concept and will, in collaboration with CTO and support from key providers like Adobe and Microsoft, deliver training programs for County personnel focused on transformative learning that will enable them to most effectively utilize the capabilities and functionality of software and services in which the County is investing.

Our approach to providing IT services to the County has always been to deliver the right solution at the best price, in line with County's strategic objectives. Our commitment is to build on that approach. We have strong relationships with top tier providers including EMC, Oracle and IBM. Whether a technology comes from a strategic partner or a perceived competitor, we will bring the best solution to the County to achieve the best business outcome. The delivery of reliable, predictable and quality results, with high end-user satisfaction, is of utmost importance to us. We are pleased to note that together with County CTO, we achieved the highest rating to date in the annual Gartner IT customer satisfaction survey, reaching the top category, "Best in Class".

Operational excellence requires the pursuit of continuous improvement. At all levels across our organization, our focus on problem solving, teamwork and leadership will ensure we consistently identify and seize opportunities to provide optimal results. The transformative specifics in our proposal provide mechanisms the County can leverage to foster new ways of thinking and spark creativity among our teams across the County, industry partners, and constituents. We will ensure a sound foundation from which the County can address current challenges as well as provide services to the next generation resident - one who is proactive, connected, and aspiring to contribute. Like the County, we believe that "Good Government Demands the Intelligent Interest of Every Citizen" and we will collaborate with the

County to identify and implement technologies and programs to encourage that interest, and enable every citizen to be engaged.

Building on the vision established by the CTO, HPES developed a local Innovation Council. The council's charter is to address real business needs, increase efficiency and reduce County spend. Once a year, we host Innovation Day at the COC for all interested County users where these innovation ideas are showcased. Since 2014, the Innovation Council has presented 26 ideas, 10 of which have been implemented into production. These solutions have had a positive impact on County users and citizen-centric services.

HPES is honored to be a Live Well San Diego partner. Our commitment to the community is also demonstrated through engagements like election night support, fielding a team for the Live Well San Diego 5K, sponsoring and attending the State of the County address, and providing speakers and technical support for County events such as Passport to Life Career & Education Expo and the Dick Wayman Technology Center Ribbon Cutting Ceremony at the Ramona Library. At numerous other County events you will find the employees of HPES and our partner AT&T in the mix; participating, supporting and occasionally sponsoring. We are engaged and involved on a personal level.

And for good reason: We live here. Our highly qualified team is primarily comprised of San Diego County residents. We understand what we do matters, to our families, our friends, our neighbors, and the entire San Diego region.

You will see many familiar names in our list of 20 Key Personnel; individuals who have worked shoulder to shoulder with the County delivering consistent results, solving problems and building a relationship of trust. The team will continue to be led by Cathy Varner, our current and proposed Account Executive, who has been supporting the County since 2006. Our telecommunications partner, AT&T, will continue to be led by Grant Morgan, who has also supported the County for 10 years. Together, our team has a broad set of skills uniquely suited to supporting the County. From architects and engineers to service desk and desk side support, we are steadfast in our commitment. We are knowledgeable of County business and culture and we demonstrate that knowledge in every aspect of our performance.

It has been a privilege for HPES to support the County's IT and Telecommunications for the past 10 years. We do not take for granted the trust the County has placed in us. Our core tenet has been and will continue to be, "we must earn the opportunity to do business with the County". As the incumbent, our knowledge and experience presents the lowest risk transition. We will continue to consistently deliver the County's IT operations while we transition and transform to the technologies required by the new scope of work and beyond.

The new frontier for our partnership will be a model of excellence in reliability, continuous improvement, transformation, and strategic alignment, advancing the gauge for County staff, constituents, and visitors.

As we move forward in our partnership, you can be assured that your reputation as the best managed local government in America will continue to be affirmed.

Table of Contents

Executive Summary ..... **i**
3. Pricing **1**
3.1 Volume III Checklist 2
3.2 Offeror Responses to Pricing Questionnaire 3
3.3 Terms & Conditions 4
3.4 Financial Position 5
3.4.1 Prime Contractor Financial Information 5
3.4.2 Subcontractor Financial Information 5
3.5 Resource Unit Pricing 6
3.5.1 Pricing Concepts 6
3.5.2 Resource Unit Fee Modification 15
3.5.3 Third-Party Applications 16
3.5.4 Three-Tiered Resource Unit Approach 16
3.5.5 Applications Services 17
3.5.6 Pricing Appendix 18
3.6 Assumptions 19
3.7 Offeror Response to Pricing Exceptions 20
3.8 Appendix 21
HPES 3-year Audited Financials 22
AT&T 3-year Audited Financials 49
Exhibit Z: Schedule 16.1 Fees 74
Exhibit AA: Exhibit 16.1-1 Resource Unit Price Summary 75
Exhibit CC: Exhibit 16.1-2 Resource Unit Price Decomposition 76
Exhibit DD: Exhibit 16.1-3 Maximum Annual Fee 77
Exhibit FF: Exhibit 16.1-5 Firm Fixed Price for Applications M&O 78
Exhibit GG: Exhibit 16.1-5b Firm Fixed Price for Applications M&O 79

3. Pricing

3.1 Volume III Checklist

Proposal Item	Offeror Agrees to Meet?	
Item 1: Offeror's agrees to meet all the requirements in SCHEDULE 16.1 FEES provided. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 2: Offeror's must complete and submit EXHIBIT 16.1-1 RESOURCE UNIT PRICE SUMMARY provided. The Offeror must check "Yes" on indicating compliance, or "No" on the non-compliance with the requirement.	YES ☒	NO ☐
Item 3: Offeror's must complete and submit EXHIBIT 16.1-2 RESOURCE UNIT PRICE DECOMPOSITION provided. The Offeror must check "Yes" on indicating compliance, or "No" on the non-compliance with the requirement.	YES ☒	NO ☐
Item 4: Offeror's must complete and submit EXHIBIT 16.1-3 MAXIMUM ANNUAL FEE provided. The Offeror must check "Yes" on indicating compliance, or "No" on the non-compliance with the requirement.	YES ☒	NO ☐
Item 5: Offeror's must complete and submit EXHIBIT 16.1-5 FIRM FIXED PRICE FOR APPLICATIONS M&O provided. The Offeror must check "Yes" on indicating compliance, or "No" on the non-compliance with the requirement.	YES ☒	NO ☐
Item 6: Offeror's must complete and submit EXHIBIT 16.1-5B FIRM FIXED PRICE FOR APPLICATIONS M&O provided. The Offeror must check "Yes" on indicating compliance, or "No" on the non-compliance with the requirement.	YES ☒	NO ☐
Item 7: Offeror agrees to meet all the requirements in EXHIBIT 16.1-4 LABOR CATEGORIES FEE provided. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 8: Offeror agrees to meet all the requirements in EXHIBIT 16.8 FEE REDUCTIONS provided. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 9: Offeror agrees to meet all the requirements in SCHEDULE 3.2 FORM BILL OF SALE provided. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐
Item 10: Offeror agrees to meet all the requirements in Schedule 16.7 – BENCHMARKING METHODOLOGY. The Offeror must check "Yes" indicating agreement, or "No" indicating non-agreement with the requirements.	YES ☒	NO ☐

3.2 Offeror Responses to Pricing Questionnaire

Section left blank intentionally to maintain document structure.

3.3 Terms & Conditions

ITEM #	TECHNICAL REFERENCE (SECTION, PAGE, PARAGRAPH)	EXCEPTION (SHORT DESCRIPTION OF TEXT OR REQUIREMENT)	OFFEROR PROPOSED SOLUTION/RATIONALE AND BENEFITS OF PROPOSED SOLUTION TO THE COUNTY	EXCEPTION AMOUNT

The following table represents our proposed Termination for Convenience during Transition. These amounts would be offset by any payments received against Transition Milestones.

Table 1. Termination Fees by Month

MONTH	AMOUNT
1	$ 1,222,912
2	$ 2,485,663
3	$ 3,936,137
4	$ 5,585,573
5	$ 7,488,248
6	$ 9,279,999
7	$ 10,252,618
8	$ 11,163,589
9	$ 12,172,527

3.4 Financial Position

3.4.1 Prime Contractor Financial Information

Attached are Hewlett Packard Enterprise's (HPE) 2013, 2014, and 2015 Annual Reports. We extracted the audited financial sections from each report so they are concise, economical, and easy to find. Upon request, we will be happy to provide electronic pdf files or complete hard copies of HPE financial reports for the past 3 years. Please note that the total three years information is over 650 pages.

A complete copy of the 2013 HP Annual Report can be found here:
http://h30261.www3.hp.com/~/media/Files/H/HP-IR/documents/reports/2014/hpq-annual-report-2013.pdf

A complete copy of the 2014 HP Annual Report can be found here:
http://h30261.www3.hp.com/~/media/Files/H/HP-IR/documents/reports/2015/hpq-annual-report-2014.pdf

On November 1, 2015, HP Enterprise Service' former corporate parent, the Hewlett-Packard Company (HPCo), separated into two publicly traded Fortune 50 companies. One company consists of HPCo's enterprise technology infrastructure, software, and services businesses and is now an independent, publicly traded company, the Hewlett Packard Enterprise Company (HPE). The other company, HP Inc., (formerly known as Hewlett-Packard Company) consists of HPCo's printing and personal systems businesses and retains the HP logo. As part of the planning for this transaction, HPCo took steps to maintain the strength and reliability of HP Enterprise Services, LLC, and other entities.

HP Enterprise Services, LLC (HPES, LLC) is a fully owned subsidiary of Hewlett Packard Enterprise Company (HPE). HPE is well capitalized with high, investment-grade credit ratings.

A complete copy of the 2015 Hewlett Packard Enterprise Annual Report can be found here:
http://proxy.investors.hpe.com/~/media/Files/H/HPE-Proxy/documents/proxy-statement-2015-annual-report.pdf.

3.4.1.2. Provide your organization's annual revenue for the past three (3) years.

Hewlett Packard Enterprise's annual net revenue for the past three 3 years as shown in Table 1 (2013 and 2014 reflect annual revenue of our predecessor company, Hewlett Packard Company prior to separation).

Table 2. Hewlett Packard Enterprise's Annual Net Revenue

2013	2014	2015
$112.298 billion	$111.454 billion	$52.107 billion

3.4.2 Subcontractor Financial Information

Please see attachments for AT&T's Annual Reports for 2013, 2014, and 2015. We extracted the audited financial sections from each report so they are concise, economical, and easy to find. Upon request, we will be happy to provide electronic pdf files or complete hard copies of AT&T's financial reports for the past 3 years. Please note that the total three years information is over 300 pages.

3.4.2.2. Provide each subcontractor's annual revenue for the past three (3) years.

AT&T's annual operating revenue is shown in Table 3.

Table 3. AT&T's Annual Operating Revenue

2013	2014	2015
$128.752 billion	$132.447 billion	$146.801 billion

3.5 Resource Unit Pricing

3.5.1 Pricing Concepts

HPES has used the pricing template as defined in Exhibits 16.1-1 as the basis for pricing. In the section below, HPES provides insight into the pricing concepts we used to develop the Resource Unit (RU) pricing.

Cross-Functional

For the Cross-Functional services, we performed a bottom-up pricing effort to build up the per month price. The major cost drivers for each RU are listed below:

- Contract and Acquisition Management Services – Basis includes all resources who perform contract and subcontract management, as well as those who perform acquisition (procurement) services.
- Integrated Asset Management Services – Basis includes all resources performing asset management services. Tool costs, which are driven by volume, are associated with the appropriate RU.
- Billing Management Services – Basis includes resources who perform billing management services, billing, and charge back/invoicing services associated with the appropriate RU.
- Security Management Services – Includes all resources, tools, and core infrastructure providing security management services. This also includes response to the annual audit request that we provide today. Security Management Services costs, which are driven by volume, are associated with the appropriate RU.
- Service Delivery Management Services – Basis is the Service Delivery Managers listed in the key personnel section of the technical proposal.
- Project Management Services – Project Management Office (PMO) for intake and governance of applications and infrastructure work requests. HPES has also taken this opportunity to offer additional value to the CoSD customer by consolidating Infrastructure Project Management efforts, which were previously part of the monthly server RUs, into our project management service. This will provide value to our customer while continuing to facilitate HPES's goal to integrate all project management services under one set of best practices.
- Integration and Testing Services – Engineering resources who perform integration and testing services in support of infrastructure services.
- Incident Management Services – Resources to manage governance of processes for Incident Management.
- Problem Management Services – Resources to manage governance of processes for Problem Management.
- Change Management Services – Resources to manage governance of processes for Change Management.
- Release Management Services – Resources to manage governance of processes for Release Management.
- Configuration Management – Resources to manage governance of processes for Configuration Management.
- Capacity Planning and Performance Management Services – Resources to manage governance of processes for Capacity Planning, and Capacity and Performance Management.
- Disaster Recovery (DR) Management Services – Basis includes the resources who maintain DR plans and coordinate DR tests and network connectivity, as well as the subscription cost to cover all of the infrastructure required to provide Disaster Recovery environments for those applications that have designated Recovery Time and Recovery Point Objectives as of this submission. The subscriptions costs include the following: Per server costs based on size of server, storage costs charged per TB, Continuous Data Protection, Network Infrastructure costs, Internet bandwidth, and DR exercise coordination. As DR requirements and application infrastructure composition changes, this RU will be revisited. As an alternative pricing structure for DR, to provide greater flexibility, HPES suggests

the County consider using this RU to cover the cost of planning, testing, and network services only, and then create a set of RUs to cover the incremental per server and storage Disaster Recovery subscription services. This would more accurately reflect usage and results in savings to the County. In addition, this alternative pricing structure will align with the County's goal that changes in scale will be addressed via volume changes rather than RU changes.

- Identity Access Management (IDAM) Services – Basis is resources and tools providing the IDAM service, including Symantec PKI and the Oracle IDAM Platform support. This includes maintenance of end-user accounts, password resets, and managing permissions.
- Reporting Management Services – Basis is the resources who manage the process to produce and publish reports, and meet with the County to review, refine, and identify new requirements.
- Domain Name Management Services – Basis is the resources to provide management of Domain Names.
- Business Analyst Services – Basis is five Full-Time Equivalents (FTEs) to provide the services as described.
- Chief Technical Architect Services – Basis is one FTE (Key Personnel) to provide the services as described.
- Enterprise Applications Architect Services – Basis is one FTE (Key Personnel) to provide the Services as described.
- Innovation Management Services – Basis is one FTE (Key Personnel) to serve as Innovation Officer.
- The basis for the breakdown of the Cross Functional Resource Units is based on the labor and tools required to provide each service.

Service Desk

HPES has priced this RU to support the HPES-proposed service levels at the current call volumes actual cost reflects an average with an anticipated reduction built in based on self service.

End User

All of the End-User Services RUs include hardware, software, and resources to support each type of platform. Refresh has been included at the required intervals and the price includes the remaining lease cost from the existing contract. The subscription costs for Office 365 is included in our pricing.

The following RUs have additional information:

- Mobile Device Support Services – Resources and tools to support mobile devices.
- Early Refresh - Mobile PC and Early Refresh - Desktop – This RU contains the sum of the future hardware decomposition fees (remaining lease).
- County Retained Device, Desktop – DCSS, Laptop - DCSS – These RUs include the software and resources to support the device, with no hardware component or refresh.

Network

HPES has teamed with AT&T to continue to provide fast, highly secure mobile connectivity and network services to the County.

Network Access – Static Wired Service is provided on a fixed monthly fee per active account. Unit pricing includes the cabling and switching systems (5-year refresh), routing (4-year refresh), security (4-year refresh), Wide Area Network (WAN) circuits, Internet access, and VTC QOS/infrastructure access.

Network Access – Wired/Wireless – Unit prices provided are per active account and include cabling, switching systems (5-year refresh), routing (4-year refresh), security (4-year refresh), WAN circuits, Internet access, VTC QOS/infrastructure access, and wifi secured access. Additional unit pricing is provided for units that are greater or less than 10% above or below the baseline volume band provided.

Virtual Private Network (VPN) Access Level 1 is provided on a fixed monthly fee per access. Unit pricing includes SSL VPN infrastructure and licensing, maintenance and support, to enable network persistent, secure access.

Virtual Private Network (VPN) Access Level 2 - Basis is the software maintenance and support cost for application persistence. This RU is an optional uplift to Network Access Wire/Wireless, and cannot be purchased as a stand-alone. Note that new users will need to order a license as a one-time purchase from the OIC.

Voice Services are provided on a fixed monthly fee per unit. Units proposed include seconds, calls, phones (for pay phones), active lines, and active accounts. There are no charges for on- and off-net resource units (calls) supported by PBX/VoIP services. The following voice services are individually priced (except where noted).

- Calls – Casual Use – Calls not originated as direct dial or inbound requiring special handling charges, including operator-assisted calls both inbound and outbound
- Calls – Conference Bridge – Conference Bridge support
- Calls – Directory Assistance – charges apply to 411 dialed calls only
- Calls – International – charges apply to direct dialed international calls only
- Calls – Off-Net Local – No charges
- Calls: Off-Net Toll – No charges
- Calls – Off-Net Long Distance (CA) – No charges
- Calls – Off-Net Long Distance (USA) – No charges
- Calls – On-Net – No charges
- Calls – 800 Service (CA) – Prices provided are for PBX/VoIP supported sites
- Calls – Toll Free 800 (San Diego and Imperial) – Prices provided are for PBX/VoIP supported sites
- Calls – Toll Free 800 (USA) – Prices provided are for PBX/VoIP supported sites
- Pay Phones – Prices provided are per phone per month and include PSTN circuit connection and cabling. Pay phones are coin/card operated and owned by the provider (not a County retained/purchased asset)
- Voice – Analog Line – Unit prices provided are per active line and include telephone set break-fix support, ATA/Gateways (to support VoIP environment), circuit and BVoIP infrastructure to eliminate outbound direct distance dialing usage charges for domestic calls. Existing telephones will be used as much as possible.
- Voice – Single Line – Unit prices provided are per active line and include telephone set break-fix support, Gateways for PSTN connectivity, circuits, and BVoIP infrastructure to eliminate outbound direct distance dialing usage charges associated with domestic calls. Existing VoIP telephones will be used as much as possible and will replace TDM-based phones and cabling (Cat 3 to Cat 5E as required).
- Voice – Multi-Line – Unit prices provided are per active line and include telephone set break-fix support, Gateways for PSTN connectivity, circuits, and BVoIP infrastructure to eliminate outbound direct distance dialing usage charges associated with domestic calls. Existing VoIP telephones will be used as much as possible and will replace TDM-based phones and cabling (Cat 3 to Cat 5E as required).
- Voicemail – Unit prices provided are per active account and include Unified Communications (UC) capabilities of integration with UC services from multiple manufacturers. Includes geo redundant architecture with no single point of failure.
- Voicemail to Email Services – Unit prices provided are per active account and include service administration and support, and cloud-based licensing and maintenance/support for the Mutare service. Available to all voice single-line, multi-line subscribers.

- **Interactive Voice Services** – Unit prices provide include infrastructure (hardware and software), circuitry, and limited software development of the IVS applications. Additional charges will apply should external databases/systems require access or custom development. Unit prices are based on complexity of the service and features utilized. Three RU categories have been defined: Small, Medium and Large.
- **Interactive Voice Services** – Support for County Retained – Unit prices provided include trunking and PSTN connectivity to County owned IVS systems not included in this Agreement.

Video Conferencing Services – Unit prices provided are per system and include codec and head end infrastructure, software, and administration needed to support and maintain services. Two categories of VTC have been priced, Room System Video Teleconferencing Services and Personal Video Teleconferencing Services.

The Bluejeans integrated video teleconferencing offer included in this proposal includes a 100 host license, where designated video conferencing hosts will be identified by the County. Additional licensing options are available up to an enterprise scale, allowing all users on the County domain the ability to host a multi-platform video conference. The Bluejeans service has been allocated across the Network Access RU and will not have a separate price point. Changes to this licensing model could materially impact the RU price offered under this solution.

Town Hall Services – Unit prices provided includes 12+ VM Servers with Storage Area Network and 4 Video Network Edge appliances (CDN) and AVMS/QUMU application license and VNE/CDN licenses with a 5 year refresh cycle. Labor includes Application, Content Distribution and Portal support, Townhall administrator and Portal updates. Origination and distribution bandwidth and Originator connectivity limited to available facilities.**Video Streaming and Archiving** – Unit prices provided are per system and include access and circuitry for the existing Granicus webcasting solution at the current subscribed level.

Wireless Access Point (WAP) – Unit prices provided are per access point and include support, LAN andconnectivity, equipment, and infrastructure required to install and maintain wireless access points at official County sites. Outdoor WAPs are included; however, mounts and cabling are limited to "on existing building." Additional unit pricing is provided for units that are greater or less than 10% above or below the baseline volume band provided.

Third-Party Network Access Services – Unit prices provided are fixed monthly prices for the associated network. Pricing includes leased-line-based access to the County data network, administration, maintenance, support, cross-connects, DMZ, and firewall interface for a third-party-provided leased line in the AT&T POP. The following third-party network access services are leased-line-based:

- Category 1
- Category 2
- Category 3.

The following third-party network access services are Internet based and include access via ISP and peering configuration on firewall in the AT&T POP, administration, maintenance, and support:

- IP Sec (5 Mbps)
- IP Sec (10 Mbps)

The following third-party network access services are virtual and include access for third parties occupying County facilities and providing access to either external services or specified County access via the firewall. Prices include administration, support, and maintenance.

- Virtual Access (1 Mbps)
- Virtual Access (2 Mbps)
- Virtual Access (3 Mbps)
- Virtual Access (4 Mbps)
- Virtual Access (5 Mbps)
- Virtual Access (6-10 Mbps)
- Virtual Access (20 Mbps)
- Virtual Access (30 Mbps)
- Virtual Access (40 Mbps)
- Virtual Access (50 Mbps)

External DNS Management – Unit prices are fixed monthly fees per unit and include all administration and support of the Akamai Fast DNS Cloud Solution.

New Site Installation Services – Unit prices are fixed rates that can be decoupled based on the County's selection of optional services. The following are the new installation services provided and priced:

- Base services (the fixed component), will include activities such as pre-field work and requirements gathering, network design, circuit design/provisioning, installation of network hardware and project management that are required regardless of the cabling vendor used.
- The optional services (the variable component), will include all cabling vendor activities as well as contractor project management oversight. These optional components are broken into two work categories in an effort to allow the County to select either all or a subset of the cabling work necessary at the new site. The first component within the optional services will be identified as "Riser Cabling". This component will include the placement of pathway and rack infrastructure as well as the placement and testing of fiber/copper based cabling runs between MPOE and MDF, and between MDF and IDF rooms/floors. Trenching is not included in this service and will be the obligation of the County or its contractor to provide. The second optional component of the service will be identified as "Horizontal Cabling". Included in this service will be the placement and testing of all wall jacks, patch panels and plenum cabling between the IDF and the workstations or designated end points.
- Should the County elect to move one or both of these optional service components to a vendor of their choice, the resource unit will be decomposed to provide adequate cost recovery for the remaining New Site services.

Data Center

The basis of the RU pricing for Data Center Services follows:

- Mainframe – Basis is the cost to continue operating the current workload on the current mainframe environment without refresh (per CPU hour).
- Physical Servers – Basis is all hardware, software, tools, and support resources for a physical server. Sizing is based on the current definitions in Report 49.
- Virtual Guest Servers – Basis includes support resources and an allocation of certain hardware/software, tools, and facilities costs to run the environment. The cost of hardware and software for the physical host on which the virtual guest resides is priced separately as either a medium or a large UNIX server.

As an alternative to the current approach, HPES suggests creating sized RUs for Virtual Servers similar to Physical Servers (Extra-Small, Small, Medium, Large, Extra-Large). This would permit the cost of the physical server infrastructure to be allocated equitably into the Virtual Servers based on how much resource each Virtual consumes. Physical infrastructure would be automatically ordered and added as needed to support expansion of the Virtual Server environment without the County having to order and fund these servers explicitly.

- AS/400 – Basis is the cost to continue operating the current server without refresh.
- Infrastructure Services – Basis includes all hardware, software, network, facility, and support resources to manage the services explicitly listed in Schedule 4.3, Section 6.8. These services include WAN Acceleration, Load Balancing, core Data Center Network elements (firewalls, switches, all Servers and Storage used to support underpinning services (such as Active Directory, Distributed File Systems, ADFS, . A portion of the MPC costs associated with supporting the infrastructure have been allocated to this RU.
- Development and Test Environment – Basis includes all hardware, software, network, and labor to support non-production environments used for new development projects. A portion of the MPC environment, calculated based on the current mix of Development vs M&O infrastructure, is allocated to this RU.

  There are two alternative pricing approaches that the County may wish to consider. Either or a combination of both may be applied at the County's discretion:
  - Include the infrastructure and support for the on-demand managed private cloud in this RU, and all other development/test environments (anything not cloud compatible) would be funded on a per-server basis as they are today.
  - Include all Applications M&O environments in this RU, so that as applications move from development to M&O, the environments used for them do not have to change in their accounting/reporting structure – this would prevent the scenario of potentially having to re-price both RUs when a large application moves into production.
- Email Services – Basis is licensing and resources supporting the email portion of Office 365 with Exchange Online Advanced Threat Protection and Archiving. It also includes hardware, software, and support resources for Data Loss Prevention, RightFax™, and SMTP relay. Because encryption is included in the service, Email Encryption Services are not separately priced. Also included is the cost of HPES Enhanced Support for Office 365, which is a bridge service between the HPES Service Desk and Microsoft Support.
- Office 365 Network Enabler – This new Service has been added as a New Capability in Exhibit 16-1.1. The basis for the price is Netbond and MS Azure ExpressRoute service for Office 365 connectivity.

Storage

Storage RU does not include Disaster Recovery, storage in the Disaster Recovery site is covered by the Disaster Recovery Cross-Functional RU. Under the current tier definitions, any tier may also be presented as Network Attached Storage.

- Attached Storage – WINTEL- Basis is 1 GB of direct-attached storage, RAID – Protected.
- Attached Storage – UNIX - Basis is one GB of direct-attached storage, RAID – Protected.
- Storage - Document Processing Center (DPC) – Basis is one 5 TB dedicated storage array, and all hardware, software, and support resources for the server environment supporting this service. This also includes the cost of replication and VTL-based backups under current retention requirements.
- Storage - Primary Tier – Basis is hardware, software, and support resources for 1 GB 3PAR storage (SSD +10K drives), thick provisioned in the highest performing RAID configuration. This also includes the cost of VTL-based backups under current retention requirements.

- Storage - Secondary Tier – Basis is hardware, software, and support resources for 1 GB 3PAR storage (10K drives), thin provisioned. This also includes the cost of VTL-based backups under current retention requirements.
- Storage - Archive Tier – Basis is hardware, software, and support resources for 1 GB 3PAR storage (7200 RPM drives), thin provisioned. This also includes the cost of VTL-based backups under current retention requirements.
- Storage - Immutable Tier (1 TB) – Basis is hardware, software, and support resources to manage 1 TB storage on an EMC Centera or similar technology.
- Storage - Immutable Tier (500 GB) – Basis is hardware, software, and support resources to manage 500 GB storage on an EMC Centera or similar technology.

Print

- Print per 1,000 images (Paper) – Basis is printer hardware and software, forms, materials, and support resources to manage the centralized Print Services environment (per 1,000 images)
- Microfiche Originals – Basis is service to create fiche, support resources, and materials to manage the service.
- Microfiche Duplicates – Basis is service to duplicate fiche, support resources, and materials to manage the service.

Third-Party Agreements

Please refer to Section 3.5.4, Three-Tiered Resource Unit Approach, in this volume, for a description of these RUs.

Application Services

Applications Development Time and Materials (T&M) hours represent 1 hour of time for a person who meets the qualifications as defined in Exhibit EE/16.1-4, Labor Categories. Application Maintenance and Operations Services include resources and the development/test tools to support the environment. The pricing developed for Exhibit FF: Exhibit 16.1-5, Firm Fixed Price for Applications M&O includes all infrastructure, including a portion of the MPC, used to support this activity. The price does not include the effort for the Applications marked as retired in Exhibit 16.1-5 Applications.

Based on the hours included in Exhibit AA: Exhibit 16.1-1, Resource Unit Price Summary, price sheets, it appears the hours for Applications Maintenance and Operations support are also included in the evaluation volumes, and that Exhibit FF: Exhibit 16.1-5, Firm Fixed Price for Applications M&O, would duplicate the costs.

Transition Services

Each framework transition includes the cost to make process changes, develop new reports, update existing reports, set-up to measure and report new or modified service levels and post artifacts to the service portal. One-time costs to implement specific projects are included in the frameworks as required by Schedule 2.1, Transition Services, as listed below:

- Transition Services – Service Desk Framework – Resources and tools cost to implement the Service Portal.
- Transition Services – Application Services Framework - Resources to transition the SaaS applications.
- Transition Services – End-User Services Framework – No projects required.
- Transition Services – Network Services Framework - No projects required.

- Transition Services - Data Center Services Framework – Consolidation to one data center, implementation of new DR strategy and infrastructure, migration to MS Office 365, implementation of the on-demand Development and Test Environment, Storage Architecture.
- Transition Services – Cross-Functional Services Framework – Implementation of component-level management plans, and implementation of new DR Plans, Service Levels, Reporting, and Security requirements for the other Frameworks. The Cross Functional transition also includes some specific initiatives:
  - replacement of myRequests
  - implementation of the Application Performance Management Suite of tools (this is included in Cross Functional because it crosses and supports multiple frameworks)
  - Implementation of a number of Identity Management capabilities required by the Statement of Work.
- Transition Services – Transition Completion – No additional projects required.

Transformation Services

All transformation activities described include those projects specifically requested. All pricing provided is based on high-level assumptions and a notional project scope. As requirements are received, we will validate or refine the solution accordingly. Basis information for these projects follows.

- Desktop Services – Basis is infrastructure, software, and labor to implement and support an Application Virtualization environment for a widely used candidate application, such as Kronos. We estimated a starting user base of 200, with per-user pricing beyond that volume. A possible alternative would be to implement a small-scale pilot first, then develop a design targeted for specific applications.
- User Data Services – Basis is enhanced support for OneDrive for Business on a per-user basis. Data encryption in transit and at rest is included; however, no uplifted security or data protection design has been applied, beyond the native file versioning available from Microsoft.
- IT Application Portfolio Management Services – Basis is resources, hardware, and software to implement a project to implement the Mega tool, including consultants to install, customize, and configure the IT Portfolio Management Plus Solution - Advanced Edition solution and train HPES and County users. Notional solution basis (license volume) is:
  - One WorkBench User (Solutions)
  - One Administrator User (Solutions)
  - 30 ITPM Plus Solution - Contributors
  - 10 ITPM Plus Solution - Portfolio Manager - Advanced Edition Users
  - 5 ITPM Plus Solution - Portfolio Manager Users
- Network Transformation – Basis is AT&T Netbond dedicated, scalable, secure connection service to a third-party cloud provider. The following tiers are offered:
  - NetBond 1 Mbps
  - NetBond 3 Mbps
  - NetBond 10 Mbps
  - NetBond 25 Mbps
  - NetBond 40 Mbps
  - NetBond 100 Mbps
  - NetBond 155 Mbps
  - NetBond 300 Mbps
  - NetBond 600 Mbps
  - NetBond 800 Mbps
  - NetBond 1,000 Mbps
  - NetBond 2,000 Mbps
  - NetBond 3,000 Mbps

  - NetBond 4,000 Mbps
  - NetBond 5,000 Mbps

Note that connectivity to each cloud provider will require both a NetBond component and that cloud provider's equivalent.

- Voice Services Transformation – Included in Network Base Services under the Voice RU's. Not separately priced.
- Storage Architecture – Basis includes implementation and ongoing management of the ControlPoint software environment, based on an estimated 100 TB of unstructured data, and a pilot implementation (one-time cost only) of Structured Data Management. There are numerous other types of storage that could be offered for the County's consideration.
- E911 – Included in Network Base Services under the Voice RU's. Not separately priced.
- Identity Federated Services – Basis is tiered pricing for HPES Identity and Access Management as a Service (IAMaaS). Based on actual expected user volumes, we can modify the tier structure.
  - Identity Federated Services - up to 50k bundle
  - Identity Federated Services - up to 100k bundle
  - Identity Federated Services - up to 150k bundle
  - Identity Federated Services - up to 250k bundle
  - Identity Federated Services - up to 500k bundle
  - Identity Federated Services - up to 999k bundle
  - Identity Federated Services - up to 1,500k bundle

Two additional projects were suggested in the transformation volume of this proposal:

- Enterprise Information Management (EIM) – a consulting engagement focused on defining the vision and strategy for EIM as well as documenting the roadmap for subsequent implementation.
- Comprehensive Applications Threat Analysis (CATA) Services – these services can be ordered in the following ways:

  - Standard CATA Review includes a Security Requirements Gap Analysis (SRGA) and Architectural Threat Analysis (ATA) for one Application Architecture, for that Application's first review.
  - Delta CATA Review includes the same services as a Standard CATA Review, for one Application Architecture, for subsequent reviews, due to (for example) application changes or changes in security policy. A Standard CATA Review must have been completed at some previous time.
  - Time and Materials – Rates are provided for Strategist, Master, and Expert levels. These rates may be used for code assessments, application vulnerability assessments, and Penetration Testing, or other application security services, as required.

Additional or Alternative Resource Units

Hybrid Cloud Environment Add-On RUs - The following optional resource units are offered for the County's consideration. These are add-ons to the hybrid cloud environment, and cannot be implemented independently. Pricing for these options includes the ability to provision and monitor the instances, and does not include the cost of the instance resources themselves, nor underlying infrastructure as noted in the sub-bullets.

- Option to provision virtual server environments in Amazon Web Services or Microsoft Azure public or Government clouds.
  - Cost of Netbond-type connectivity will be priced and offered separately once the County's bandwidth requirement for this service is determined.

- Option to provision Oracle VM Server for SPARC VMs in the Tulsa Data Center.
  - Cost of underlying infrastructure (Oracle physical servers and operating software) would be priced separately as part of the underlying resource units' infrastructure, as with traditionally hosted environments

Disaster Recovery (DR) Management Services RUs - To assist with one of the County's goals of having changes in scale addressed through volume changes, HPES is proposing an alternative RU structure for the Disaster Recovery (DR) Management Services. HPES proposes the following RU's:

- DR Labor – Represents the Labor to manage and update DR process and plans. This RU also contains the labor for DR Exercise Coordination and providing Exercise Collateral.
- DR Infrastructure – Represents the Hardware, Software, and Labor to support the DR Infrastructure. This costs includes the cost of the BRS Site Service Charge, Base Network and circuit costs, Recovery Management and Configuration Servers, and 100MBPs Internet Bandwidth.
- DR Small Windows/Linux – 72 Hour RTO – Represents the server subscription price for small physical servers. Servers falling under this band will contain 1-2 cores and includes ProLiant BL460, and PowerEdge 2850s.
- DR Medium Windows/Linux – 72 Hour RTO – Represents the server subscription price for medium physical servers. Servers falling under this band will contain 4-8 cores include ProLiant BL660, and PowerEdge 1950s.
- DR Large Windows/Linux – 72 Hour RTO – Represents the server subscription price for large physical servers. Servers falling under this band will contain 8-16 cores.
- DR X-Large Windows/Linux – 72 Hour RTO – Represents the server subscription price for extra large physical servers. Servers falling under this band will contain greater than 16 cores and includes ProLiant DL580e G9 or the equivalent.
- DR Medium Solaris – 72 Hour RTO – Represents the server subscription price for small physical servers. Servers falling under this band will contain 16 cores and includes SPARC T4-1 or SPARC T4-4
- DR Large Solaris – 72 Hour RTO – Represents the server subscription price for small physical servers. Servers falling under this band will contain 16-32 cores and includes SPARC Enterprise M5000
- DR X-Large Solaris – 72 Hour RTO – Represents the server subscription price for small physical servers. Servers falling under this band includes SPARC Enterprise M3000
- DR VTL Based Storage – 72 Hour RTO – Includes the hardware, software and labor support for VTL storage.
- DR Small Virtual – 48 Hour RTO - Represents the server subscription price for small physical servers. Servers falling under this band will contain 1-2 cores
- DR Medium Virtual – 48 Hour RTO Represents the server subscription price for small physical servers. Servers falling under this band will contain 4 cores
- DR Large Virtual – 48 Hour RTO Represents the server subscription price for small physical servers. Servers falling under this band will contain 8 cores
- DR 3PAR Based Storage – 48 Hour RTO – Includes the hardware, software and labor support for storage. Includes Continuous Data Protection.

3.5.2 Resource Unit Fee Modification

HPES has provided the banded pricing as defined in Exhibit BB:Exhibit 16.1-1a, Fees Sample Calculation.

3.5.3 Third-Party Applications

Under the Applications M&O Services, these 169 cloud-based applications have been included as M&O bundles in Exhibit FF. HPES will create help desk scripts as required for Tier 1 support. The application information will be entered and maintained in the applications CMDB.

Cloud-Based Retained Assets can be submitted for transfer to HPES as third-party software using the existing County and HPES Contract Transfer Request Form. Cloud-Based Retained Assets transferred as Third-Party Software will incur the Third-Party Agreement fees.

3.5.4 Three-Tiered Resource Unit Approach

HPES is proposing the following pricing tiers based on our experience supporting the County of San Diego as shown in Table 4. . These fees are applicable as defined in Schedule 16.1-1, Section 8.1.1 and distinct from the Contract and Acquisition Management Services resource unit.

Table 4. Pricing Tiers

RESOURCE UNIT	FEE	DESCRIPTION
Third Party – Tier 1	$10,000 per occurrence	Negotiation of an agreement with a New Third-Party Vendor, as defined below,in excess of $500,000
Third Party – Tier 2	$5,000 per occurrence	Negotiation of an agreement with a New Third-Party Vendor up to $500,000
Third Party – Tier 3	5% of transaction amount with a minimum fee of $100 and maximum fee of $50,000	Fee applied to the below transactions for products and services which are not provided by services for which Contractor is paid a Resource Unit Fee • Portfolio Software - Perpetual License Purchase • Portfolio Software - Perpetual License Maintenance Renewal • Portfolio Software - SaaS Subscription Licenses Purchase/Renewal • Portfolio Software - Cloud/ASP Subscription • Labor SOW • Labor Agency Contractor • Hardware • Hardware Maintenance

Tier 1 or Tier 2 is assessed on execution of a signed contract between HPES and the New Third-Party Vendor. A New Third-Party Vendor is defined as a vendor with whom HPE does not have a current agreement applicable to the transaction, whether never existed or expired, for which new terms and conditions must be negotiated.

Tier 3 is assessed, in addition to Tier 1 or Tier 2 if those are applicable, upon receipt of invoices from third-party vendor. The Tier 3 fee is assessed on the total transaction amount including shipping costs and taxes.

Below are examples of the application of above Resource Units:

- County requests HPES to contract with company AAA for labor services in the amount of $100,000. Company AAA is a third-party vendor currently contracted by HPES in support of the Services.

The total fees are:

- (1) "Third Party – Tier 3" for 5% of transaction amount of $100,000 equaling $5,000.

- County requests HPES to contract and purchase software licenses from company BBB. Company BBB is not a third-party vendor currently contracted by HPES in support of the Services. The vendor price of the software is $80,000 plus $20,000 for the first year of software maintenance.

The fees are:

- (1) "Third Party – Tier 2" for $5,000 plus
- (1) "Third Party – Tier 3" for 5% of transaction amount of $100,000 equaling $5,000.

Total fees are $10,000.

1. County requests HPES to transact a software maintenance renewal from company BBB Company. Company BBB is a third-party vendor currently contracted by HPES in support of the Services. The vendor price for the software maintenance renewal is $20,000.

The total fees are:

- (1) "Third Party – Tier 3" for 5% of transaction amount of $20,000 equaling $1,000.

2. County requests HPES to purchase a large scanner not available in the OIC catalog or as a Resource Unit. The price of the scanner is $10,000. The scanner can be purchased by HPES through a third-party vendor currently contracted by HPES in support of the Services.

The total fees are:

- "Third Party – Tier 3" for 5% of transaction amount of $10,000 equaling $500.

The following table shows County's historical third-party spend through the ITO Contract, including licenses, license maintenance, ISRs (labor, hardware), and the OIC catalog.

Table 5. Historical ITO Third-Party Resale Spend

HISTORICAL ITO THIRD-PARTY RESALE SPEND

Period: May 2011 - June 2016						
In $000's						
	FY Ending June 30, 2011	FY Ending June 30, 2012	FY Ending June 30, 2013	FY Ending June 30, 2014	FY Ending June 30, 2015	FY Ending June 30, 2016
3rd Party COTS Licenses	90	2,292	5,038	4,310	4,430	3,077
3rd Party COTS Maint	826	7,805	12,493	9,822	10,875	10,856
Individual Service Request	1,489	5,514	7,755	7,819	5,993	5,398
OIPC Catalog	344	1,816	1,850	1,439	1,708	1,627
Grand Total	2,749	17,427	27,137	23,389	23,005	20,957

3.5.5 Applications Services

Left blank intentionally

3.5.6 Pricing Appendix

See Appendix 3.8, Exhibit AA: Exhibit 16.1-1 Resource Unit Price Summary, and Exhibit CC: Exhibit 16.1-2, Resource Unit Price Decomposition, for required exhibit.

3.5.6.3. Complete and submit in Microsoft Word Exhibit 16.1-3 Maximum Annual Fee as follows:

See Appendix 3.8, Exhibit DD: Exhibit 16.1-3 Maximum Annual Fee, for required exhibit.

3.5.6.4. Complete and submit in Microsoft Excel Exhibit 16.1-5 Fixed Price for Applications Maintenance & Operations as follows based on instructions in the 'Exhibit 16.1-5 Questions' tab.

See Appendix 3.8, Exhibit FF: Exhibit 16.1-5 Firm Fixed Price for Applications M&O, for required exhibit.

3.5.6.5. Complete and submit in Microsoft Word Exhibit 16.1-5b Fixed Price for Applications Maintenance & Operations as follows:

See Appendix 3.8, Exhibit GG: Exhibit 16.1-5b Firm Fixed Price for Applications M&O, for required exhibit.

3.6 Assumptions

ITEM #	REFERENCE (SECTION, PAGE, PARAGRAPH)	DESCRIPTION	RATIONALE
1.	General	The County and HPES will execute a letter agreement regarding Telecom Transport Services similar to the existing agreement dated 4/12/2011 or otherwise incorporate such changes into the RFP terms and conditions prior to contract signature.	This will support HPES compliance with Federal law regarding certain regulated telecommunications services and allow for more favorable pricing to the County

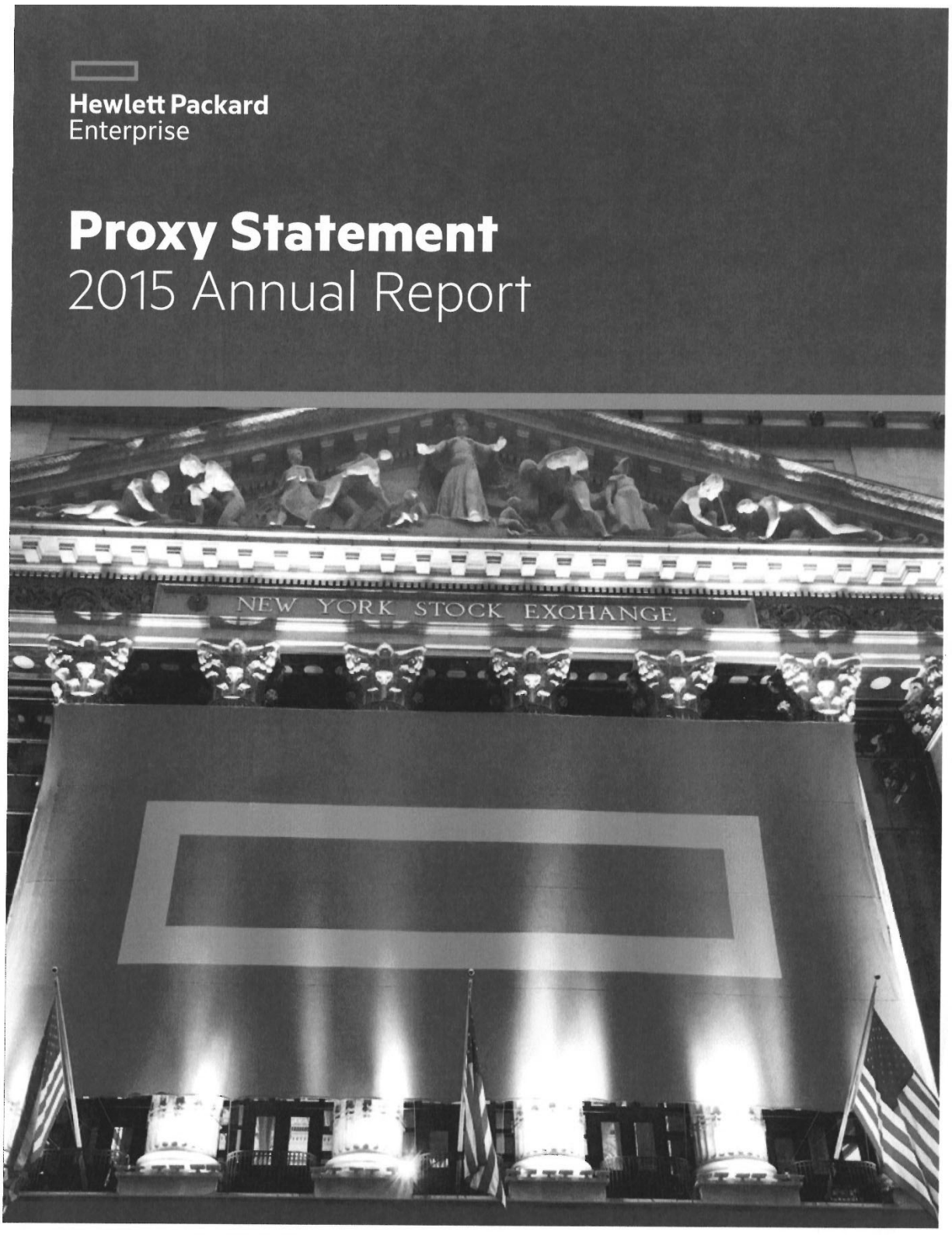
3.7 Offeror Response to Pricing Exceptions

ITEM #	REFERENCE (SECTION, PAGE, PARAGRAPH)	EXCEPTION	OFFEROR PROPOSED SOLUTION/RATIONALE AND BENEFITS OF PROPOSED SOLUTION TO THE COUNTY
1.			
2.			
3.			

HPES has no pricing exceptions.

3.8 Appendix

HPES 3-year Audited Financials


Hewlett Packard
Enterprise
Proxy Statement
2015 Annual Report
NEW YORK STOCK EXCHANGE

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of Hewlett Packard Enterprise Company

We have audited the accompanying combined and consolidated balance sheets of Hewlett Packard Enterprise Company and subsidiaries (the "Company") as of October 31, 2015 and 2014, and the related combined and consolidated statements of earnings, comprehensive income, cash flows, and equity for each of the three years in the period ended October 31, 2015. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. We were not engaged to perform an audit of the Company's internal control over financial reporting. Our audits included consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control over financial reporting. Accordingly, we express no such opinion. An audit also includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements, assessing the accounting principles used and significant estimates made by management, and evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the combined and consolidated financial position of Hewlett Packard Enterprise Company and subsidiaries at October 31, 2015 and 2014, and the combined and consolidated results of their operations and their cash flows for each of the three years in the period ended October 31, 2015, in conformity with U.S. generally accepted accounting principles.

/s/ ERNST & YOUNG LLP

San Jose, California
December 17, 2015

HEWLETT PACKARD ENTERPRISE COMPANY AND SUBSIDIARIES

Combined and Consolidated Statements of Earnings

	For the fiscal years ended October 31		
	2015	2014	2013
	In millions, except per share amounts		
Net revenue:			
Products	$19,635	$19,171	$19,383
Services	32,111	35,551	37,541
Financing income	361	401	447
Total net revenue	52,107	55,123	57,371
Costs and expenses:			
Cost of products	12,978	12,394	12,360
Cost of services	23,950	26,815	28,958
Financing interest	240	277	312
Research and development	2,338	2,197	1,956
Selling, general and administrative	8,025	8,717	8,601
Amortization of intangible assets	852	906	1,228
Restructuring charges	954	1,471	983
Acquisition and other related charges	89	11	21
Separation costs	797	—	—
Defined benefit plan settlement charges	225	—	—
Impairment of data center assets	136	—	—
Total costs and expenses	50,584	52,788	54,419
Earnings from operations	1,523	2,335	2,952
Interest and other, net	(53)	(91)	(81)
Earnings before taxes	1,470	2,244	2,871
Benefit (provision) for taxes	991	(596)	(820)
Net earnings	$ 2,461	$ 1,648	$ 2,051
Net earnings per share[1]:			
Basic	$ 1.36	$ 0.91	$ 1.14
Diluted	$ 1.34	$ 0.90	$ 1.12
Number of shares used to compute net earnings per share[1]:			
Basic	1,804	1,804	1,804
Diluted	1,834	1,834	1,834

(1) On November 1, 2015, HP Inc. (formerly Hewlett-Packard Company) distributed a total of 1.8 billion shares of Hewlett Packard Enterprise common stock to HP Inc. stockholders as of the record date. The number of shares used to compute basic and diluted net earnings per share ("EPS") for the period ended October 31, 2015 is used for the calculation of net EPS for all periods presented. See Note 16, "Net Earnings Per Share", for further details.

The accompanying notes are an integral part of these Combined and Consolidated Financial Statements.

HEWLETT PACKARD ENTERPRISE COMPANY AND SUBSIDIARIES

Combined and Consolidated Statements of Comprehensive Income

	For the fiscal years ended October 31		
	2015	2014	2013
	In millions		
Net earnings	$ 2,461	$1,648	$2,051
Other comprehensive (loss) income before taxes:			
Change in unrealized (losses) gains on available-for-sale securities:			
Unrealized (losses) gains arising during the period	(10)	5	44
Gains reclassified into earnings	—	(1)	(49)
	(10)	4	(5)
Change in unrealized gains (losses) on cash flow hedges:			
Unrealized gains arising during the period	481	111	36
(Gains) losses reclassified into earnings	(480)	60	(53)
	1	171	(17)
Change in unrealized components of defined benefit plans:			
(Losses) gains arising during the period	(382)	(794)	115
Amortization of actuarial loss and prior service benefit	214	82	86
Curtailments, settlements and other	4	18	9
Plans transferred from Parent during the period	(2,607)	—	—
Merged into Parent's Shared plans during the period	—	61	142
	(2,771)	(633)	352
Change in cumulative translation adjustment	(198)	(85)	(150)
Other comprehensive (loss) income before taxes	(2,978)	(543)	180
Benefit (provision) for taxes	211	(10)	(76)
Other comprehensive (loss) income, net of taxes	(2,767)	(553)	104
Comprehensive (loss) income	$ (306)	$1,095	$2,155

The accompanying notes are an integral part of these Combined and Consolidated Financial Statements.

HEWLETT PACKARD ENTERPRISE COMPANY AND SUBSIDIARIES

Combined and Consolidated Balance Sheets

	As of October 31	
	2015	2014
	In millions	
ASSETS		
Current assets:		
Cash and cash equivalents	$ 9,842	$ 2,319
Accounts receivable	8,538	8,423
Financing receivables	2,918	2,974
Inventory	2,198	1,884
Other current assets	7,677	6,431
Total current assets	31,173	22,031
Property, plant and equipment	9,886	8,520
Long-term financing receivables and other assets	11,020	6,503
Goodwill	27,261	25,960
Intangible assets	1,930	2,057
Total assets	$81,270	$65,071
LIABILITIES AND EQUITY		
Current liabilities:		
Notes payable and short-term borrowings	$ 691	$ 894
Accounts payable	5,828	4,889
Employee compensation and benefits	2,902	2,737
Taxes on earnings	634	706
Deferred revenue	5,154	5,129
Accrued restructuring	628	711
Other accrued liabilities	6,314	4,694
Total current liabilities	22,151	19,760
Long-term debt	15,103	485
Other liabilities	10,098	7,654
Commitments and contingencies		
Equity:		
Parent company investment	38,550	39,024
Retained earnings	—	—
Accumulated other comprehensive loss	(5,015)	(2,248)
Equity attributable to the Company	33,535	36,776
Non-controlling interests	383	396
Total equity	33,918	37,172
Total liabilities and equity	$81,270	$65,071

The accompanying notes are an integral part of these Combined and Consolidated Financial Statements.

HEWLETT PACKARD ENTERPRISE COMPANY AND SUBSIDIARIES

Combined and Consolidated Statements of Cash Flows

	For the fiscal years ended October 31		
	2015	2014	2013
	In millions		
Cash flows from operating activities:			
Net earnings	$ 2,461	$ 1,648	$ 2,051
Adjustments to reconcile net earnings to net cash provided by operating activities:			
Depreciation and amortization	3,947	4,144	4,396
Stock-based compensation expense	565	427	374
Provision for doubtful accounts	52	80	81
Provision for inventory	155	125	161
Restructuring charges	954	1,471	983
Deferred taxes on earnings	(2,522)	(304)	(248)
Excess tax benefit from stock-based compensation	(100)	(44)	(1)
Other, net	376	11	325
Changes in operating assets and liabilities, net of acquisitions:			
Accounts receivable	9	986	580
Financing receivables	(393)	428	478
Inventory	(424)	69	(251)
Accounts payable	868	611	472
Taxes on earnings	956	404	532
Restructuring	(1,021)	(1,239)	(733)
Other assets and liabilities	(2,222)	(1,906)	(461)
Net cash provided by operating activities	3,661	6,911	8,739
Cash flows from investing activities:			
Investment in property, plant and equipment	(3,344)	(3,620)	(2,497)
Proceeds from sale of property, plant and equipment	380	606	370
Purchases of available-for-sale securities and other investments	(243)	(940)	(938)
Maturities and sales of available-for-sale securities and other investments	298	1,023	1,005
Payments made in connection with business acquisitions, net of cash acquired	(2,644)	(49)	(167)
Proceeds from business divestitures, net	140	6	—
Net cash used in investing activities	(5,413)	(2,974)	(2,227)
Cash flows from financing activities:			
Short-term borrowings with original maturities less than 90 days, net	(39)	18	(121)
Issuance of debt	866	852	1,083
Payment of debt	(1,077)	(1,135)	(2,200)
Net transfers from (to) Parent	9,440	(3,542)	(5,196)
Issuance of Senior Notes relating to separation	14,546	—	—
Distribution of net proceeds of Senior Notes relating to separation to Parent	(14,529)	—	—
Cash dividends paid to non-controlling interests	(32)	(37)	(31)
Excess tax benefit from stock-based compensation	100	44	1
Net cash provided by (used in) financing activities	9,275	(3,800)	(6,464)
Increase in cash and cash equivalents	7,523	137	48
Cash and cash equivalents at beginning of period	2,319	2,182	2,134
Cash and cash equivalents at end of period	$ 9,842	$ 2,319	$ 2,182
Supplemental cash flow disclosures:			
Income taxes paid, net of refunds	$ 192	$ 302	$ 354
Interest expense paid	$ 291	$ 357	$ 374
Supplemental schedule of non-cash investing and financing activities:			
Net transfers of property, plant and equipment from Parent	$ 1,788	$ —	$ —

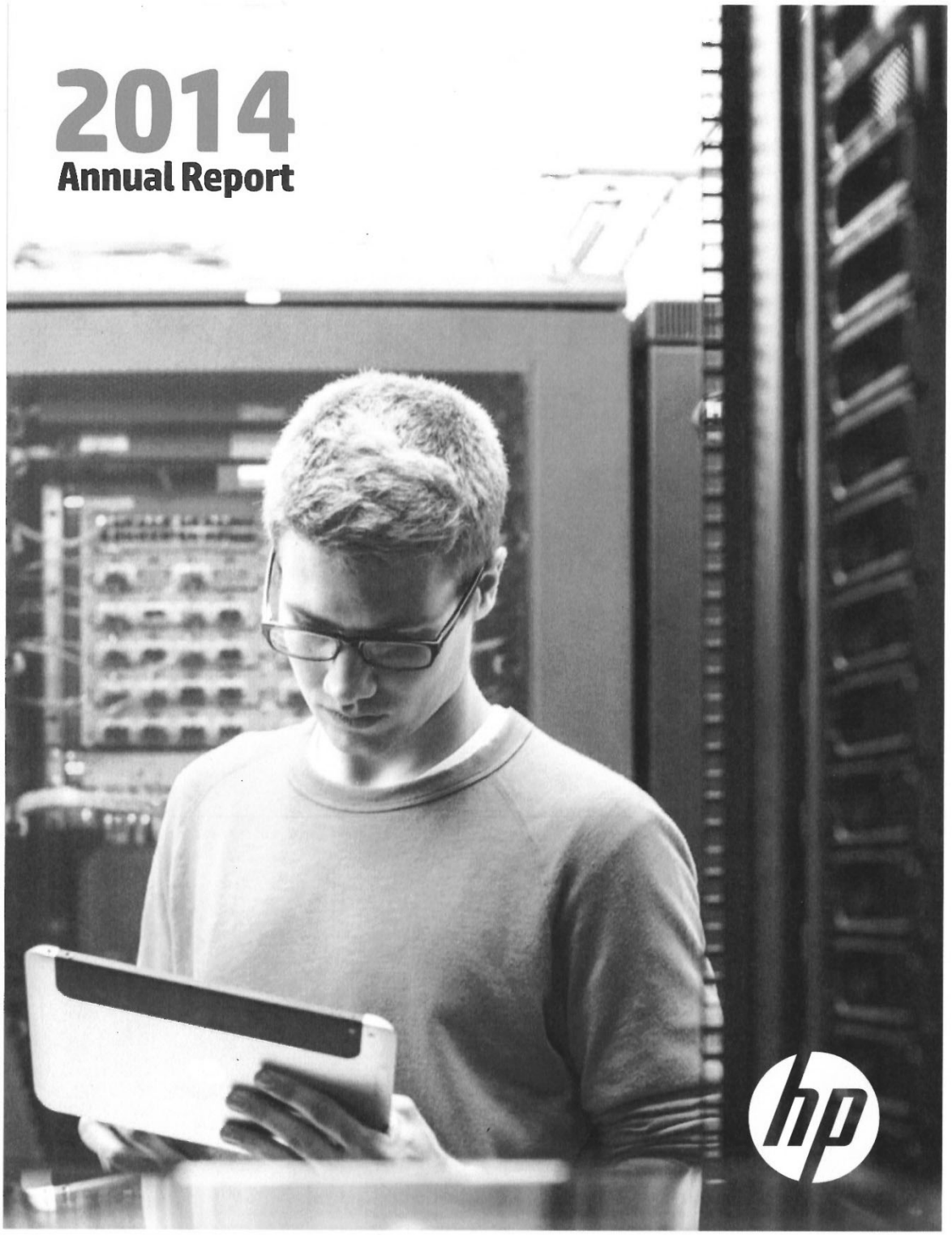
The accompanying notes are an integral part of these Combined and Consolidated Financial Statements.

HEWLETT PACKARD ENTERPRISE COMPANY AND SUBSIDIARIES

Combined and Consolidated Statements of Equity

	Parent Company Investment	Accumulated Other Comprehensive Loss	Equity Attributable to the Company	Non-controlling Interests	Total Equity
			In millions		
Balance at October 31, 2012	$ 40,971	$(1,799)	$ 39,172	$397	$ 39,569
Net earnings	2,051		2,051		2,051
Other comprehensive income		104	104		104
Comprehensive income			2,155		2,155
Net transfers to Parent	(3,339)		(3,339)		(3,339)
Changes in non-controlling interests				(10)	(10)
Balance at October 31, 2013	39,683	(1,695)	37,988	387	38,375
Net earnings	1,648		1,648		1,648
Other comprehensive loss		(553)	(553)		(553)
Comprehensive income			1,095		1,095
Net transfers to Parent	(2,307)		(2,307)		(2,307)
Changes in non-controlling interests				9	9
Balance at October 31, 2014	39,024	(2,248)	36,776	396	37,172
Net earnings	2,461		2,461		2,461
Other comprehensive loss		(2,767)	(2,767)		(2,767)
Comprehensive income			(306)		(306)
Net transfers from Parent	11,594		11,594		11,594
Distribution of net proceeds of Senior Notes to Parent	(14,529)		(14,529)		(14,529)
Changes in non-controlling interests				(13)	(13)
Balance at October 31, 2015	$ 38,550	$(5,015)	$ 33,535	$383	$ 33,918

The accompanying notes are an integral part of these Combined and Consolidated Financial Statements.


2014
Annual Report
hp

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of Hewlett-Packard Company

We have audited the accompanying consolidated balance sheets of Hewlett-Packard Company and subsidiaries as of October 31, 2014 and 2013, and the related consolidated statements of earnings, comprehensive income, stockholders' equity, and cash flows for each of the three years in the period ended October 31, 2014. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the consolidated financial position of Hewlett-Packard Company and subsidiaries at October 31, 2014 and 2013, and the consolidated results of their operations and their cash flows for each of the three years in the period ended October 31, 2014, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), Hewlett-Packard Company's internal control over financial reporting as of October 31, 2014, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (1992 framework) and our report dated December 17, 2014 expressed an unqualified opinion thereon.

/s/ ERNST & YOUNG LLP

San Jose, California
December 17, 2014

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of Hewlett-Packard Company

We have audited Hewlett-Packard Company's internal control over financial reporting as of October 31, 2014, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (1992 framework) (the COSO criteria). Hewlett-Packard Company's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Management's Report on Internal Control Over Financial Reporting. Our responsibility is to express an opinion on the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, Hewlett-Packard Company maintained, in all material respects, effective internal control over financial reporting as of October 31, 2014, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the accompanying consolidated balance sheets of Hewlett-Packard Company and subsidiaries as of October 31, 2014 and 2013, and the related consolidated statements of earnings, comprehensive income, stockholders' equity and cash flows for each of the three years in the period ended October 31, 2014 and our report dated December 17, 2014 expressed an unqualified opinion thereon.

/s/ ERNST & YOUNG LLP

San Jose, California
December 17, 2014

Management's Report on Internal Control Over Financial Reporting

HP's management is responsible for establishing and maintaining adequate internal control over financial reporting for HP. HP's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with U.S. generally accepted accounting principles. HP's internal control over financial reporting includes those policies and procedures that (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of HP; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of HP are being made only in accordance with authorizations of management and directors of HP; and (iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of HP's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

HP's management assessed the effectiveness of HP's internal control over financial reporting as of October 31, 2014, utilizing the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in Internal Control—Integrated Framework (1992 framework). Based on the assessment by HP's management, we determined that HP's internal control over financial reporting was effective as of October 31, 2014. The effectiveness of HP's internal control over financial reporting as of October 31, 2014 has been audited by Ernst & Young LLP, HP's independent registered public accounting firm, as stated in their report which appears on page 82 of this Annual Report on Form 10-K.

/s/ MARGARET C. WHITMAN

Margaret C. Whitman
Chairman, President and Chief Executive Officer
December 17, 2014

/s/ CATHERINE A. LESJAK

Catherine A. Lesjak
Executive Vice President and Chief Financial Officer
December 17, 2014

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Earnings

	For the fiscal years ended October 31		
	2014	2013	2012
	In millions, except per share amounts		
Net revenue:			
Products	$ 73,726	$ 72,398	$ 77,887
Services	37,327	39,453	42,008
Financing income	401	447	462
Total net revenue	111,454	112,298	120,357
Costs and expenses:			
Cost of products	56,469	55,632	59,468
Cost of services	28,093	30,436	32,600
Financing interest	277	312	317
Research and development	3,447	3,135	3,399
Selling, general and administrative	13,353	13,267	13,500
Amortization of intangible assets	1,000	1,373	1,784
Impairment of goodwill and intangible assets	—	—	18,035
Restructuring charges	1,619	990	2,266
Acquisition-related charges	11	22	45
Total operating expenses	104,269	105,167	131,414
Earnings (loss) from operations	7,185	7,131	(11,057)
Interest and other, net	(628)	(621)	(876)
Earnings (loss) before taxes	6,557	6,510	(11,933)
Provision for taxes	(1,544)	(1,397)	(717)
Net earnings (loss)	$ 5,013	$ 5,113	$(12,650)
Net earnings (loss) per share:			
Basic	$ 2.66	$ 2.64	$ (6.41)
Diluted	$ 2.62	$ 2.62	$ (6.41)
Weighted-average shares used to compute net earnings (loss) per share:			
Basic	1,882	1,934	1,974
Diluted	1,912	1,950	1,974

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Comprehensive Income

	For the fiscal years ended October 31		
	2014	2013	2012
	In millions		
Net earnings (loss)	$ 5,013	$5,113	$(12,650)
Other comprehensive (loss) income before taxes:			
Change in unrealized gains on available-for-sale securities:			
Unrealized gains arising during the period	7	52	25
Gains reclassified into earnings	(1)	(49)	—
	6	3	25
Change in unrealized gains (losses) on cash flow hedges:			
Unrealized gains (losses) arising during the period	337	(243)	335
Losses (gains) reclassified into earnings	151	106	(399)
	488	(137)	(64)
Change in unrealized components of defined benefit plans:			
(Losses) gains arising during the period	(2,756)	1,953	(2,457)
Amortization of actuarial loss and prior service benefit	259	326	172
Curtailments, settlements and other	51	25	122
	(2,446)	2,304	(2,163)
Change in cumulative translation adjustment	(85)	(150)	(47)
Other comprehensive (loss) income before taxes	(2,037)	2,020	(2,249)
(Provision) benefit for taxes	(66)	(239)	188
Other comprehensive (loss) income, net of taxes	(2,103)	1,781	(2,061)
Comprehensive income (loss)	$ 2,910	$6,894	$(14,711)

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Balance Sheets

	As of October 31	
	2014	2013
	In millions, except par value	
ASSETS		
Current assets:		
Cash and cash equivalents	$ 15,133	$ 12,163
Accounts receivable	13,832	15,876
Financing receivables	2,946	3,144
Inventory	6,415	6,046
Other current assets	11,819	13,135
Total current assets	50,145	50,364
Property, plant and equipment	11,340	11,463
Long-term financing receivables and other assets	8,454	9,556
Goodwill	31,139	31,124
Intangible assets	2,128	3,169
Total assets	$103,206	$105,676
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities:		
Notes payable and short-term borrowings	$ 3,486	$ 5,979
Accounts payable	15,903	14,019
Employee compensation and benefits	4,209	4,436
Taxes on earnings	1,017	1,203
Deferred revenue	6,143	6,477
Accrued restructuring	898	901
Other accrued liabilities	12,079	12,506
Total current liabilities	43,735	45,521
Long-term debt	16,039	16,608
Other liabilities	16,305	15,891
Commitments and contingencies		
Stockholders' equity:		
HP stockholders' equity		
Preferred stock, $0.01 par value (300 shares authorized; none issued)	—	—
Common stock, $0.01 par value (9,600 shares authorized; 1,839 and 1,908 shares issued and outstanding at October 31, 2014 and October 31, 2013, respectively)	18	19
Additional paid-in capital	3,430	5,465
Retained earnings	29,164	25,563
Accumulated other comprehensive loss	(5,881)	(3,778)
Total HP stockholders' equity	26,731	27,269
Non-controlling interests	396	387
Total stockholders' equity	27,127	27,656
Total liabilities and stockholders' equity	$103,206	$105,676

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Cash Flows

	For the fiscal years ended October 31		
	2014	2013	2012
		In millions	
Cash flows from operating activities:			
Net earnings (loss)	$ 5,013	$ 5,113	$(12,650)
Adjustments to reconcile net earnings (loss) to net cash provided by operating activities:			
Depreciation and amortization	4,334	4,611	5,095
Impairment of goodwill and intangible assets	—	—	18,035
Stock-based compensation expense	560	500	635
Provision for doubtful accounts	55	61	142
Provision for inventory	211	275	277
Restructuring charges	1,619	990	2,266
Deferred taxes on earnings	(34)	(410)	(711)
Excess tax benefit from stock-based compensation	(58)	(2)	(12)
Other, net	81	443	265
Changes in operating assets and liabilities (net of acquisitions):			
Accounts receivable	2,017	530	1,687
Financing receivables	420	484	(418)
Inventory	(580)	(4)	890
Accounts payable	1,912	541	(1,414)
Taxes on earnings	310	417	(320)
Restructuring	(1,506)	(904)	(840)
Other assets and liabilities	(2,021)	(1,037)	(2,356)
Net cash provided by operating activities	12,333	11,608	10,571
Cash flows from investing activities:			
Investment in property, plant and equipment	(3,853)	(3,199)	(3,706)
Proceeds from sale of property, plant and equipment	843	653	617
Purchases of available-for-sale securities and other investments	(1,086)	(1,243)	(972)
Maturities and sales of available-for-sale securities and other investments	1,347	1,153	662
Payments made in connection with business acquisitions, net of cash acquired	(49)	(167)	(141)
Proceeds from business divestiture, net	6	—	87
Net cash used in investing activities	(2,792)	(2,803)	(3,453)
Cash flows from financing activities:			
Short-term borrowings with original maturities less than 90 days, net	148	(154)	(2,775)
Issuance of debt	2,875	279	5,154
Payment of debt	(6,037)	(5,721)	(4,333)
Issuance of common stock under employee stock plans	297	288	716
Repurchase of common stock	(2,728)	(1,532)	(1,619)
Excess tax benefit from stock-based compensation	58	2	12
Cash dividends paid	(1,184)	(1,105)	(1,015)
Net cash used in financing activities	(6,571)	(7,943)	(3,860)
Increase in cash and cash equivalents	2,970	862	3,258
Cash and cash equivalents at beginning of period	12,163	11,301	8,043
Cash and cash equivalents at end of period	$15,133	$12,163	$ 11,301
Supplemental cash flow disclosures:			
Income taxes paid (net of refunds)	$ 1,267	$ 1,391	$ 1,750
Interest expense paid	678	837	856
Supplemental schedule of non-cash investing and financing activities:			
Purchase of assets under capital leases	$ 113	$ 3	$ 12

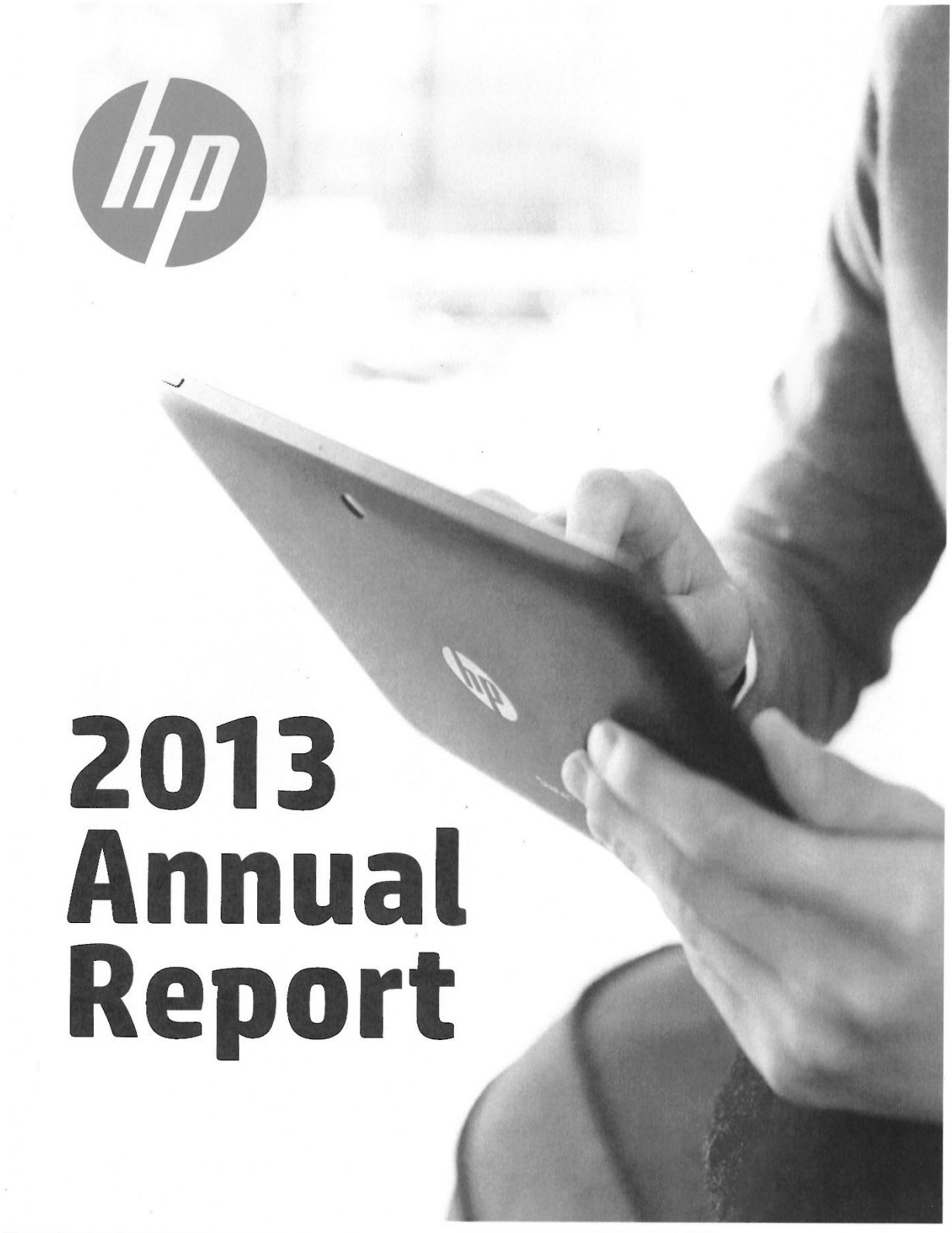
The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Stockholders' Equity

	Common Stock		Additional Paid-in Capital	Retained Earnings	Accumulated Other Comprehensive (Loss) Income	Total HP Stockholders' Equity	Non-controlling Interests	Total
	Number of Shares	Par Value						
	In millions, except number of shares in thousands							
Balance October 31, 2011	1,990,506	$20	$ 6,837	$ 35,266	$(3,498)	$ 38,625	$379	$ 39,004
Net loss				(12,650)		(12,650)		(12,650)
Other comprehensive loss					(2,061)	(2,061)		(2,061)
Comprehensive loss						(14,711)		(14,711)
Issuance of common stock in connection with employee stock plans and other	39,068		682	1		683		683
Repurchases of common stock	(66,736)		(1,525)	(101)		(1,626)		(1,626)
Tax deficiency from employee stock plans			(175)			(175)		(175)
Cash dividends declared				(995)		(995)		(995)
Stock-based compensation expense			635			635		635
Changes in non-controlling interest							18	18
Balance October 31, 2012	1,962,838	$20	$ 6,454	$ 21,521	$(5,559)	$ 22,436	$397	$ 22,833
Net earnings				5,113		5,113		5,113
Other comprehensive income					1,781	1,781		1,781
Comprehensive income						6,894		6,894
Issuance of common stock in connection with employee stock plans and other	22,950		210	(2)		208		208
Repurchases of common stock	(77,905)	(1)	(1,550)	5		(1,546)		(1,546)
Tax deficiency from employee stock plans			(149)			(149)		(149)
Cash dividends declared				(1,074)		(1,074)		(1,074)
Stock-based compensation expense			500			500		500
Changes in non-controlling interest							(10)	(10)
Balance October 31, 2013	1,907,883	$19	$ 5,465	$ 25,563	$(3,778)	$ 27,269	$387	$ 27,656
Net earnings				5,013		5,013		5,013
Other comprehensive income					(2,103)	(2,103)		(2,103)
Comprehensive income						2,910		2,910
Issuance of common stock in connection with employee stock plans and other	23,785		142	1		143		143
Repurchases of common stock	(92,380)	(1)	(2,694)	(262)		(2,957)		(2,957)
Tax deficiency from employee stock plans			(43)			(43)		(43)
Cash dividends declared				(1,151)		(1,151)		(1,151)
Stock-based compensation expense			560			560		560
Changes in non-controlling interest							9	9
Balance October 31, 2014	1,839,288	$18	$ 3,430	$ 29,164	$(5,881)	$ 26,731	$396	$ 27,127

The accompanying notes are an integral part of these Consolidated Financial Statements.


2013
Annual
Report

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of Hewlett-Packard Company

We have audited the accompanying consolidated balance sheets of Hewlett-Packard Company and subsidiaries as of October 31, 2013 and 2012, and the related consolidated statements of earnings, comprehensive income, stockholders' equity, and cash flows for each of the three years in the period ended October 31, 2013. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the consolidated financial position of Hewlett-Packard Company and subsidiaries at October 31, 2013 and 2012, and the consolidated results of their operations and their cash flows for each of the three years in the period ended October 31, 2013, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), Hewlett-Packard Company's internal control over financial reporting as of October 31, 2013, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (1992 framework) and our report dated December 27, 2013 expressed an unqualified opinion thereon.

/s/ ERNST & YOUNG LLP

San Jose, California
December 27, 2013

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of Hewlett-Packard Company

We have audited Hewlett-Packard Company's internal control over financial reporting as of October 31, 2013, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (1992 framework) (the COSO criteria). Hewlett-Packard Company's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Management's Report on Internal Control Over Financial Reporting. Our responsibility is to express an opinion on the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, Hewlett-Packard Company maintained, in all material respects, effective internal control over financial reporting as of October 31, 2013, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the accompanying consolidated balance sheets of Hewlett-Packard Company and subsidiaries as of October 31, 2013 and 2012, and the related consolidated statements of earnings, comprehensive income, stockholders' equity and cash flows for each of the three years in the period ended October 31, 2013 and our report dated December 27, 2013 expressed an unqualified opinion thereon.

/s/ ERNST & YOUNG LLP

San Jose, California
December 27, 2013

Management's Report on Internal Control Over Financial Reporting

HP's management is responsible for establishing and maintaining adequate internal control over financial reporting for HP. HP's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with U.S. generally accepted accounting principles. HP's internal control over financial reporting includes those policies and procedures that (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of HP; (ii) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of HP are being made only in accordance with authorizations of management and directors of HP; and (iii) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of HP's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

HP's management assessed the effectiveness of HP's internal control over financial reporting as of October 31, 2013, utilizing the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in Internal Control—Integrated Framework (1992 framework). Based on the assessment by HP's management, we determined that HP's internal control over financial reporting was effective as of October 31, 2013. The effectiveness of HP's internal control over financial reporting as of October 31, 2013 has been audited by Ernst & Young LLP, HP's independent registered public accounting firm, as stated in their report which appears on page 78 of this Annual Report on Form 10-K.

/s/ MARGARET C. WHITMAN

Margaret C. Whitman
President and Chief Executive Officer
December 27, 2013

/s/ CATHERINE A. LESJAK

Catherine A. Lesjak
Executive Vice President and Chief Financial Officer
December 27, 2013

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Earnings

	For the fiscal years ended October 31		
	2013	2012	2011
	In millions, except per share amounts		
Net revenue:			
Products	$ 72,398	$ 77,887	$ 84,757
Services	39,453	42,008	42,039
Financing income	447	462	449
Total net revenue	112,298	120,357	127,245
Costs and expenses:			
Cost of products	55,632	59,468	65,167
Cost of services	30,436	32,600	31,945
Financing interest	312	317	306
Research and development	3,135	3,399	3,254
Selling, general and administrative	13,267	13,500	13,577
Amortization of intangible assets	1,373	1,784	1,607
Impairment of goodwill and intangible assets	—	18,035	885
Restructuring charges	990	2,266	645
Acquisition-related charges	22	45	182
Total operating expenses	105,167	131,414	117,568
Earnings (loss) from operations	7,131	(11,057)	9,677
Interest and other, net	(621)	(876)	(695)
Earnings (loss) before taxes	6,510	(11,933)	8,982
Provision for taxes	(1,397)	(717)	(1,908)
Net earnings (loss)	$ 5,113	$(12,650)	$ 7,074
Net earnings (loss) per share:			
Basic	$ 2.64	$ (6.41)	$ 3.38
Diluted	$ 2.62	$ (6.41)	$ 3.32
Weighted-average shares used to compute net earnings (loss) per share:			
Basic	1,934	1,974	2,094
Diluted	1,950	1,974	2,128

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Comprehensive Income

	For the fiscal years ended October 31		
	2013	2012	2011
	In millions		
Net earnings (loss)	$5,113	$(12,650)	$7,074
Other comprehensive income (loss) before tax:			
Change in unrealized gains on available-for-sale securities:			
Unrealized gains arising during the period	52	25	17
Gains reclassified into earnings	(49)	—	—
	3	25	17
Change in unrealized (losses) gains on cash flow hedges:			
Unrealized (losses) gains arising during the period	(243)	335	(374)
Losses (gains) reclassified into earnings	106	(399)	658
	(137)	(64)	284
Change in unrealized components of defined benefit plans:			
Gains (losses) arising during the period	1,953	(2,457)	(289)
Amortization of actuarial loss and prior service benefit	326	172	174
Curtailments, settlements and other	25	122	2
	2,304	(2,163)	(113)
Change in cumulative translation adjustment	(150)	(47)	66
Other comprehensive income (loss) before taxes	2,020	(2,249)	254
(Provision) benefit for taxes	(239)	188	85
Other comprehensive income (loss), net of tax	1,781	(2,061)	339
Comprehensive income (loss)	$6,894	$(14,711)	$7,413

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Balance Sheets

	As of October 31	
	2013	2012
	In millions, except par value	
ASSETS		
Current assets:		
Cash and cash equivalents	$ 12,163	$ 11,301
Accounts receivable	15,876	16,407
Financing receivables	3,144	3,252
Inventory	6,046	6,317
Other current assets	13,135	13,360
Total current assets	50,364	50,637
Property, plant and equipment	11,463	11,954
Long-term financing receivables and other assets	9,556	10,593
Goodwill	31,124	31,069
Intangible assets	3,169	4,515
Total assets	$105,676	$108,768
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities:		
Notes payable and short-term borrowings	$ 5,979	$ 6,647
Accounts payable	14,019	13,350
Employee compensation and benefits	4,436	4,058
Taxes on earnings	1,203	846
Deferred revenue	6,477	7,494
Accrued restructuring	901	771
Other accrued liabilities	12,506	13,500
Total current liabilities	45,521	46,666
Long-term debt	16,608	21,789
Other liabilities	15,891	17,480
Commitments and contingencies		
Stockholders' equity:		
HP stockholders' equity		
Preferred stock, $0.01 par value (300 shares authorized; none issued)	—	—
Common stock, $0.01 par value (9,600 shares authorized; 1,908 and 1,963 shares issued and outstanding, respectively)	19	20
Additional paid-in capital	5,465	6,454
Retained earnings	25,563	21,521
Accumulated other comprehensive loss	(3,778)	(5,559)
Total HP stockholders' equity	27,269	22,436
Non-controlling interests	387	397
Total stockholders' equity	27,656	22,833
Total liabilities and stockholders' equity	$105,676	$108,768

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Cash Flows

	For the fiscal years ended October 31		
	2013	2012	2011
		In millions	
Cash flows from operating activities:			
Net earnings (loss)	$ 5,113	$(12,650)	$ 7,074
Adjustments to reconcile net earnings (loss) to net cash provided by operating activities:			
Depreciation and amortization	4,611	5,095	4,984
Impairment of goodwill and intangible assets	—	18,035	885
Stock-based compensation expense	500	635	685
Provision for doubtful accounts	61	142	81
Provision for inventory	275	277	217
Restructuring charges	990	2,266	645
Deferred taxes on earnings	(410)	(711)	166
Excess tax benefit from stock-based compensation	(2)	(12)	(163)
Other, net	443	265	(46)
Changes in operating assets and liabilities (net of acquisitions):			
Accounts receivable	530	1,687	448
Financing receivables	484	(418)	(675)
Inventory	(4)	890	(1,252)
Accounts payable	541	(1,414)	275
Taxes on earnings	417	(320)	610
Restructuring	(904)	(840)	(1,002)
Other assets and liabilities	(1,037)	(2,356)	(293)
Net cash provided by operating activities	11,608	10,571	12,639
Cash flows from investing activities:			
Investment in property, plant and equipment	(3,199)	(3,706)	(4,539)
Proceeds from sale of property, plant and equipment	653	617	999
Purchases of available-for-sale securities and other investments	(1,243)	(972)	(96)
Maturities and sales of available-for-sale securities and other investments	1,153	662	68
Payments in connection with business acquisitions, net of cash acquired	(167)	(141)	(10,480)
Proceeds from business divestiture, net	—	87	89
Net cash used in investing activities	(2,803)	(3,453)	(13,959)
Cash flows from financing activities:			
Repayment of commercial paper and notes payable, net	(154)	(2,775)	(1,270)
Issuance of debt	279	5,154	11,942
Payment of debt	(5,721)	(4,333)	(2,336)
Issuance of common stock under employee stock plans	288	716	896
Repurchase of common stock	(1,532)	(1,619)	(10,117)
Excess tax benefit from stock-based compensation	2	12	163
Cash dividends paid	(1,105)	(1,015)	(844)
Net cash used in financing activities	(7,943)	(3,860)	(1,566)
Increase (decrease) in cash and cash equivalents	862	3,258	(2,886)
Cash and cash equivalents at beginning of period	11,301	8,043	10,929
Cash and cash equivalents at end of period	$12,163	$ 11,301	$ 8,043
Supplemental cash flow disclosures:			
Income taxes paid (net of refunds)	$ 1,391	$ 1,750	$ 1,134
Interest expense paid	837	856	451

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Consolidated Statements of Stockholders' Equity

	Common Stock		Additional Paid-in Capital	Retained Earnings	Accumulated Other Comprehensive (Loss) Income	Total HP Stockholders' Equity	Non-controlling Interests	Total
	Number of Shares	Par Value						
	In millions, except number of shares in thousands							
Balance October 31, 2010	2,203,898	$22	$11,569	$ 32,695	$(3,837)	$ 40,449	$332	$ 40,781
Net earnings				7,074		7,074		7,074
Other comprehensive income					339	339		339
Comprehensive income						7,413		7,413
Issuance of common stock in connection with employee stock plans and other	45,461	1	751			752		752
Repurchases of common stock	(258,853)	(3)	(6,296)	(3,669)		(9,968)		(9,968)
Tax benefits from employee stock plans			128			128		128
Cash dividends declared				(834)		(834)		(834)
Stock-based compensation expense			685			685		685
Changes in non-controlling interest							47	47
Balance October 31, 2011	1,990,506	$20	$ 6,837	$ 35,266	$(3,498)	$ 38,625	$379	$ 39,004
Net loss				(12,650)		(12,650)		(12,650)
Other comprehensive loss					(2,061)	(2,061)		(2,061)
Comprehensive loss						(14,711)		(14,711)
Issuance of common stock in connection with employee stock plans and other	39,068		682	1		683		683
Repurchases of common stock	(66,736)		(1,525)	(101)		(1,626)		(1,626)
Tax deficiency from employee stock plans			(175)			(175)		(175)
Cash dividends declared				(995)		(995)		(995)
Stock-based compensation expense			635			635		635
Changes in non-controlling interest							18	18
Balance October 31, 2012	1,962,838	$20	$ 6,454	$ 21,521	$(5,559)	$ 22,436	$397	$ 22,833
Net earnings				5,113		5,113		5,113
Other comprehensive income					1,781	1,781		1,781
Comprehensive income						6,894		6,894
Issuance of common stock in connection with employee stock plans and other	22,950		210	(2)		208		208
Repurchases of common stock	(77,905)	(1)	(1,550)	5		(1,546)		(1,546)
Tax deficiency from employee stock plans			(149)			(149)		(149)
Cash dividends declared				(1,074)		(1,074)		(1,074)
Stock-based compensation expense			500			500		500
Changes in non-controlling interest							(10)	(10)
Balance October 31, 2013	1,907,883	$19	$ 5,465	$ 25,563	$(3,778)	$ 27,269	$387	$ 27,656

The accompanying notes are an integral part of these Consolidated Financial Statements.

HEWLETT-PACKARD COMPANY AND SUBSIDIARIES

Notes to Consolidated Financial Statements

Note 1: Summary of Significant Accounting Policies

Principles of Consolidation

The Consolidated Financial Statements include the accounts of Hewlett-Packard Company ("HP") and the subsidiaries and affiliates in which HP has a controlling financial interest or is the primary beneficiary. HP accounts for equity investments in companies over which HP has the ability to exercise significant influence but does not hold a controlling interest under the equity method, and HP records its proportionate share of income or losses in Interest and other, net in the Consolidated Statements of Earnings. HP presents non-controlling interests as a separate component within Total stockholder's equity in the Consolidated Balance Sheets. Net earnings attributable to the non-controlling interests are eliminated within Interest and other, net in the Consolidated Statements of Earnings and are not presented separately as they were not material for any period presented. HP has eliminated all significant intercompany accounts and transactions.

Reclassifications and Segment Reorganization

HP has made certain segment and business unit realignments in order to optimize its operating structure. Reclassifications of certain prior-year segment and business unit financial information have been made to conform to the current-year presentation. None of the changes impacts HP's previously reported consolidated net revenue, earnings from operations, net earnings or net earnings per share. See Note 18 for a further discussion of HP's segment reorganization.

Use of Estimates

The preparation of financial statements in accordance with U.S. generally accepted accounting principles ("GAAP") requires management to make estimates and assumptions that affect the amounts reported in HP's Consolidated Financial Statements and accompanying notes. Actual results could differ materially from those estimates.

Revenue Recognition

HP derives net revenue primarily from the sale of products and services. The following revenue recognition policies define the manner in which HP accounts for sales transactions.

HP recognizes revenue when persuasive evidence of a sales arrangement exists, delivery has occurred or services are rendered, the sales price or fee is fixed or determinable, and collectibility is reasonably assured. Additionally, HP recognizes hardware revenue on sales to channel partners, including resellers, distributors or value-added solution providers at the time of delivery when the channel partners have economic substance apart from HP, and HP has completed its obligations related to the sale. HP generally recognizes revenue for its stand-alone software sales to channel partners upon receiving evidence that the software has been sold to a specific end user.

When a sales arrangement contains multiple elements, such as hardware and software products, licenses and/or services, HP allocates revenue to each element based on a selling price hierarchy. The selling price for a deliverable is based on its vendor specific objective evidence ("VSOE") of selling price, if available, third party evidence ("TPE") if VSOE of selling price is not available, or estimated selling price ("ESP") if neither VSOE of selling price nor TPE is available. HP establishes VSOE of selling price using the price charged for a deliverable when sold separately and, in rare instances, using the price established by management having the relevant authority. HP establishes TPE of selling price

AT&T 3-year Audited Financials

mobilizing our world
AT&T INC. 2013 ANNUAL REPORT

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of AT&T Inc.

We have audited the accompanying consolidated balance sheets of AT&T Inc. (the Company) as of December 31, 2013 and 2012, and the related consolidated statements of income and comprehensive income, changes in stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2013. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the consolidated financial position of the Company at December 31, 2013 and 2012, and the consolidated results of its operations and its cash flows for each of the three years in the period ended December 31, 2013, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the Company's internal control over financial reporting as of December 31, 2013, based on criteria established in Internal Control-Integrated Framework (1992 framework) issued by the Committee of Sponsoring Organizations of the Treadway Commission and our report dated February 21, 2014 expressed an unqualified opinion thereon.

Ernst & Young LLP

Dallas, Texas
February 21, 2014

Report of Independent Registered Public Accounting Firm on Internal Control over Financial Reporting

The Board of Directors and Stockholders of AT&T Inc.

We have audited AT&T Inc.'s (the Company) internal control over financial reporting as of December 31, 2013, based on criteria established in Internal Control—Integrated Framework (1992 framework) issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). The Company's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Report of Management. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of December 31, 2013, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of the Company as of December 31, 2013 and 2012, and the related consolidated statements of income and comprehensive income, changes in stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2013 and our report dated February 21, 2014 expressed an unqualified opinion thereon.

Ernst & Young LLP

Dallas, Texas
February 21, 2014

Consolidated Statements of Income

Dollars in millions except per share amounts

	2013	2012	2011
Operating Revenues	**$128,752**	$127,434	$126,723
Operating Expenses			
Cost of services and sales (exclusive of depreciation and amortization shown separately below)	**51,464**	55,228	54,904
Selling, general and administrative	**28,414**	41,066	41,314
Impairment of intangible assets	**—**	—	2,910
Depreciation and amortization	**18,395**	18,143	18,377
Total operating expenses	**98,273**	114,437	117,505
Operating Income	**30,479**	12,997	9,218
Other Income (Expense)			
Interest expense	**(3,940)**	(3,444)	(3,535)
Equity in net income of affiliates	**642**	752	784
Other income (expense) – net	**596**	134	249
Total other income (expense)	**(2,702)**	(2,558)	(2,502)
Income Before Income Taxes	**27,777**	10,439	6,716
Income tax expense	**9,224**	2,900	2,532
Net Income	**18,553**	7,539	4,184
Less: Net Income Attributable to Noncontrolling Interest	**(304)**	(275)	(240)
Net Income Attributable to AT&T	**$ 18,249**	$ 7,264	$ 3,944
Basic Earnings Per Share Attributable to AT&T	**$ 3.39**	$ 1.25	$ 0.66
Diluted Earnings Per Share Attributable to AT&T	**$ 3.39**	$ 1.25	$ 0.66

The accompanying notes are an integral part of the consolidated financial statements.

AT&T Inc. | 39

Consolidated Statements of Comprehensive Income

Dollars in millions

	2013	2012	2011
Net income	**$18,553**	$7,539	$4,184
Other comprehensive income, net of tax:			
Foreign Currency:			
Foreign currency translation adjustments (includes $(2), $0 and $(1) attributable to noncontrolling interest), net of taxes of $(78), $48 and $(117)	**(140)**	87	(219)
Reclassification adjustment included in net income, net of taxes of $30, $0 and $183	**55**	—	341
Available-for-sale securities:			
Net unrealized gains (losses), net of taxes of $137, $64, and $(21)	**257**	118	(41)
Reclassification adjustment included in net income, net of taxes of $(42), $(36) and $(29)	**(79)**	(68)	(54)
Cash flow hedges:			
Net unrealized gains (losses), net of taxes of $286, $154 and $(140)	**525**	283	(256)
Reclassification adjustment included in net income, net of taxes of $16, $15 and $8	**30**	28	15
Defined benefit postretirement plans:			
Net actuarial loss from equity method investees arising during period, net of taxes of $0, $(32) and $0	—	(53)	—
Reclassification adjustment included in net income, net of taxes of $7, $0 and $0	**11**	—	—
Net prior service credit arising during period, net of taxes of $1,695, $1,378 and $699	**2,765**	2,249	1,140
Amortization of net prior service credit included in net income, net of taxes of $(480), $(361) and $(282)	**(782)**	(588)	(460)
Other	**—**	—	1
Other comprehensive income	**2,642**	2,056	467
Total comprehensive income	**21,195**	9,595	4,651
Less: Total comprehensive income attributable to noncontrolling interest	**(302)**	(275)	(239)
Total Comprehensive Income Attributable to AT&T	**$20,893**	$9,320	$4,412

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Balance Sheets
Dollars in millions except per share amounts

	December 31,	
	2013	2012
Assets		
Current Assets		
Cash and cash equivalents	$ 3,339	$ 4,868
Accounts receivable – net of allowances for doubtful accounts of $483 and $547	12,918	12,657
Prepaid expenses	960	1,035
Deferred income taxes	1,199	1,036
Other current assets	4,780	3,110
Total current assets	23,196	22,706
Property, Plant and Equipment – Net	110,968	109,767
Goodwill	69,273	69,773
Licenses	56,433	52,352
Customer Lists and Relationships – Net	763	1,391
Other Intangible Assets – Net	5,016	5,032
Investments in and Advances to Equity Affiliates	3,860	4,581
Other Assets	8,278	6,713
Total Assets	$277,787	$272,315
Liabilities and Stockholders' Equity		
Current Liabilities		
Debt maturing within one year	$ 5,498	$ 3,486
Accounts payable and accrued liabilities	21,107	20,494
Advanced billings and customer deposits	4,212	4,225
Accrued taxes	1,774	1,026
Dividends payable	2,404	2,556
Total current liabilities	34,995	31,787
Long-Term Debt	69,290	66,358
Deferred Credits and Other Noncurrent Liabilities		
Deferred income taxes	36,308	28,491
Postemployment benefit obligation	29,946	41,392
Other noncurrent liabilities	15,766	11,592
Total deferred credits and other noncurrent liabilities	82,020	81,475
Stockholders' Equity		
Common stock ($1 par value, 14,000,000,000 authorized at December 31, 2013 and 2012: issued 6,495,231,088 at December 31, 2013 and 2012)	6,495	6,495
Additional paid-in capital	91,091	91,038
Retained earnings	31,141	22,481
Treasury stock (1,268,914,913 at December 31, 2013 and 913,836,325 at December 31, 2012, at cost)	(45,619)	(32,888)
Accumulated other comprehensive income	7,880	5,236
Noncontrolling interest	494	333
Total stockholders' equity	91,482	92,695
Total Liabilities and Stockholders' Equity	$277,787	$272,315

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Cash Flows

Dollars in millions

	2013	2012	2011
Operating Activities			
Net income	**$ 18,553**	$ 7,539	$ 4,184
Adjustments to reconcile net income to net cash provided by operating activities:			
Depreciation and amortization	**18,395**	18,143	18,377
Undistributed earnings from investments in equity affiliates	**(324)**	(615)	(623)
Provision for uncollectible accounts	**954**	1,117	1,136
Deferred income tax expense	**6,242**	1,747	2,929
Net (gain) loss from sale of investments, net of impairments	**(492)**	(19)	(89)
Impairment of intangible assets	**—**	—	2,910
Actuarial (gain) loss on pension and postretirement benefits	**(7,584)**	9,994	6,280
Changes in operating assets and liabilities:			
Accounts receivable	**(1,329)**	(1,365)	(1,164)
Other current assets	**412**	1,017	(397)
Accounts payable and accrued liabilities	**(152)**	1,798	(341)
Retirement benefit funding	**(209)**	—	(1,000)
Other – net	**330**	(180)	2,541
Total adjustments	**16,243**	31,637	30,559
Net Cash Provided by Operating Activities	**34,796**	39,176	34,743
Investing Activities			
Construction and capital expenditures:			
Capital expenditures	**(20,944)**	(19,465)	(20,110)
Interest during construction	**(284)**	(263)	(162)
Acquisitions, net of cash acquired	**(4,113)**	(828)	(2,368)
Dispositions	**1,923**	812	1,301
Sales (purchases) of securities, net	**—**	65	62
Return of advances to and investments in equity affiliates	**301**	—	—
Other	**(7)**	(1)	27
Net Cash Used in Investing Activities	**(23,124)**	(19,680)	(21,250)
Financing Activities			
Net change in short-term borrowings with original maturities of three months or less	**20**	1	(1,625)
Issuance of other short-term borrowings	**1,476**	—	—
Repayment of other short-term borrowings	**(1,476)**	—	(28)
Issuance of long-term debt	**12,040**	13,486	7,936
Repayment of long-term debt	**(7,698)**	(8,733)	(7,574)
Issuance of other long-term financing obligations	**4,796**	—	—
Purchase of treasury stock	**(13,028)**	(12,752)	—
Issuance of treasury stock	**114**	477	237
Dividends paid	**(9,696)**	(10,241)	(10,172)
Other	**251**	89	(423)
Net Cash Used in Financing Activities	**(13,201)**	(17,673)	(11,649)
Net (decrease) increase in cash and cash equivalents	**(1,529)**	1,823	1,844
Cash and cash equivalents beginning of year	**4,868**	3,045	1,201
Cash and Cash Equivalents End of Year	**$ 3,339**	$ 4,868	$ 3,045

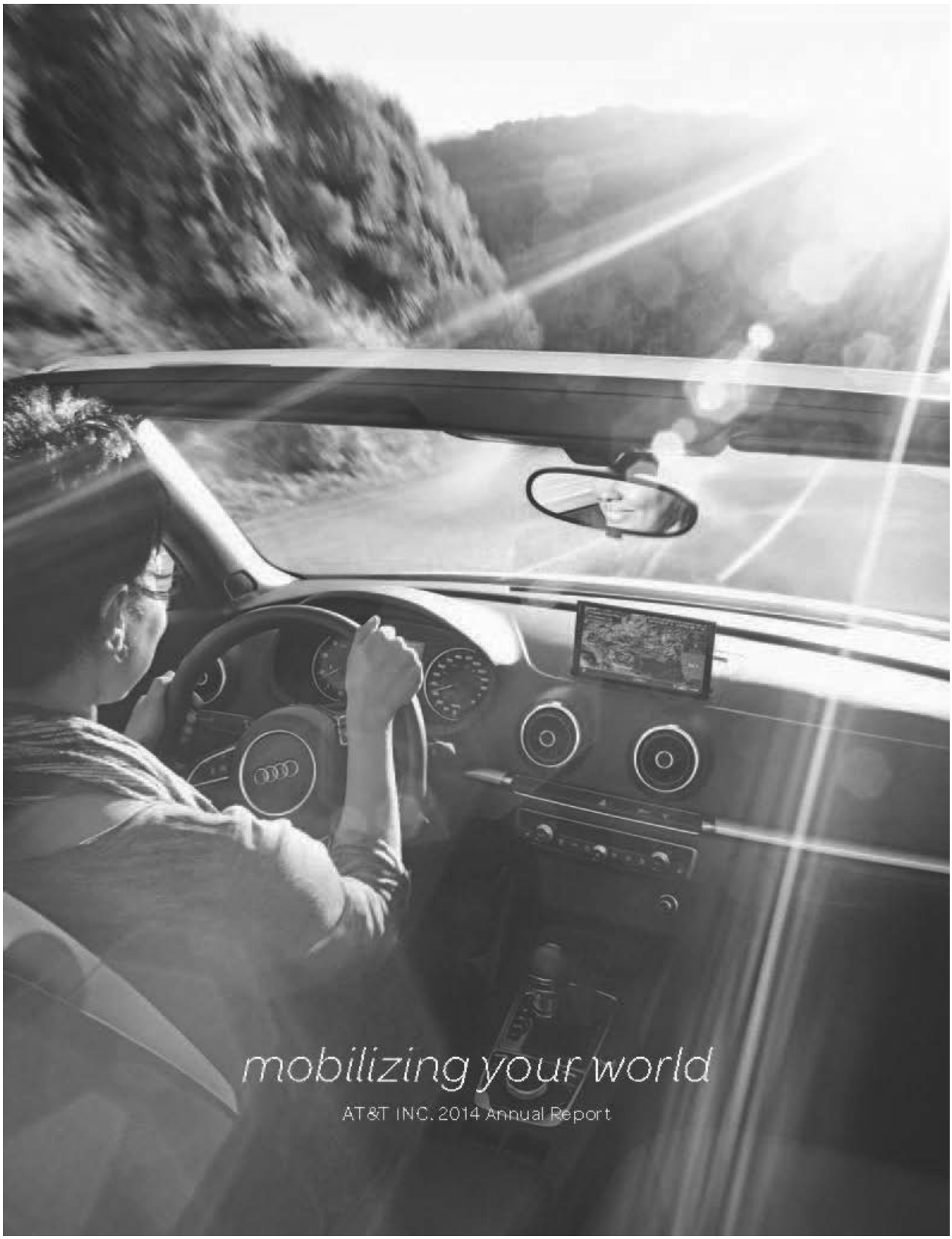
The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Changes in Stockholders' Equity

Dollars and shares in millions except per share amounts

	2013		2012		2011	
	Shares	Amount	Shares	Amount	Shares	Amount
Common Stock						
Balance at beginning of year	6,495	$ 6,495	6,495	$ 6,495	6,495	$ 6,495
Issuance of stock	—	—	—	—	—	—
Balance at end of year	6,495	$ 6,495	6,495	$ 6,495	6,495	$ 6,495
Additional Paid-In Capital						
Balance at beginning of year		$ 91,038		$ 91,156		$ 91,731
Issuance of treasury stock		(8)		120		132
Share-based payments		62		(78)		(118)
Share of equity method investee capital transactions		—		(160)		(290)
Change related to acquisition of interests held by noncontrolling owners		(1)		—		(299)
Balance at end of year		$ 91,091		$ 91,038		$ 91,156
Retained Earnings						
Balance at beginning of year		$ 22,481		$ 25,453		$ 31,792
Net income attributable to AT&T ($3.39, $1.25 and $0.66 per diluted share)		18,249		7,264		3,944
Dividends to stockholders ($1.81, $1.77 and $1.73 per share)		(9,589)		(10,236)		(10,283)
Balance at end of year		$ 31,141		$ 22,481		$ 25,453
Treasury Stock						
Balance at beginning of year	(914)	$(32,888)	(568)	$ (20,750)	(584)	$ (21,083)
Repurchase of common stock	(366)	(13,028)	(371)	(12,752)	—	—
Issuance of treasury stock	11	297	25	614	16	333
Balance at end of year	(1,269)	$(45,619)	(914)	$ (32,888)	(568)	$ (20,750)
Accumulated Other Comprehensive Income Attributable to AT&T, net of tax:						
Balance at beginning of year		$ 5,236		$ 3,180		$ 2,712
Other comprehensive income attributable to AT&T		2,644		2,056		468
Balance at end of year		$ 7,880		$ 5,236		$ 3,180
Noncontrolling Interest:						
Balance at beginning of year		$ 333		$ 263		$ 303
Net income attributable to noncontrolling interest		304		275		240
Distributions		(231)		(205)		(220)
Contributions		51		—		—
Acquisitions of noncontrolling interests		44		—		—
Acquisition of interests held by noncontrolling owners		(5)		—		(59)
Translation adjustments attributable to noncontrolling interest, net of taxes		(2)		—		(1)
Balance at end of year		$ 494		$ 333		$ 263
Total Stockholders' Equity at beginning of year		$ 92,695		$105,797		$111,950
Total Stockholders' Equity at end of year		$ 91,482		$ 92,695		$105,797

The accompanying notes are an integral part of the consolidated financial statements.


mobilizing your world
AT&T INC. 2014 Annual Report

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of AT&T Inc.

We have audited the accompanying consolidated balance sheets of AT&T Inc. (the Company) as of December 31, 2014 and 2013, and the related consolidated statements of income, comprehensive income, changes in stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2014. These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the consolidated financial position of the Company at December 31, 2014 and 2013, and the consolidated results of its operations and its cash flows for each of the three years in the period ended December 31, 2014, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the Company's internal control over financial reporting as of December 31, 2014, based on criteria established in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) and our report dated February 20, 2015 expressed an unqualified opinion thereon.

Ernst & Young LLP

Dallas, Texas
February 20, 2015

Report of Independent Registered Public Accounting Firm on Internal Control over Financial Reporting

The Board of Directors and Stockholders of AT&T Inc.

We have audited AT&T Inc.'s (the Company) internal control over financial reporting as of December 31, 2014, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) (the COSO criteria). The Company's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Report of Management. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of December 31, 2014, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of the Company as of December 31, 2014 and 2013, and the related consolidated statements of income, comprehensive income, changes in stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2014 and our report dated February 20, 2015 expressed an unqualified opinion thereon.

Dallas, Texas
February 20, 2015

Ernst & Young LLP

Consolidated Statements of Income

Dollars in millions except per share amounts

	2014	2013	2012
Operating Revenues			
Service	**$118,437**	$119,252	$118,506
Equipment	**14,010**	9,500	8,928
Total operating revenues	**132,447**	128,752	127,434
Operating Expenses			
Cost of services and sales (exclusive of depreciation and amortization shown separately below)	**60,611**	51,464	55,228
Selling, general and administrative	**39,697**	28,414	41,066
Abandonment of network assets	**2,120**	—	—
Depreciation and amortization	**18,273**	18,395	18,143
Total operating expenses	**120,701**	98,273	114,437
Operating Income	**11,746**	30,479	12,997
Other Income (Expense)			
Interest expense	**(3,613)**	(3,940)	(3,444)
Equity in net income of affiliates	**175**	642	752
Other income (expense) – net	**1,652**	596	134
Total other income (expense)	**(1,786)**	(2,702)	(2,558)
Income Before Income Taxes	**9,960**	27,777	10,439
Income tax expense	**3,442**	9,224	2,900
Net Income	**6,518**	18,553	7,539
Less: Net Income Attributable to Noncontrolling Interest	**(294)**	(304)	(275)
Net Income Attributable to AT&T	**$ 6,224**	$ 18,249	$ 7,264
Basic Earnings Per Share Attributable to AT&T	**$ 1.19**	$ 3.39	$ 1.25
Diluted Earnings Per Share Attributable to AT&T	**$ 1.19**	$ 3.39	$ 1.25

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Comprehensive Income

Dollars in millions

	2014	2013	2012
Net income	**$6,518**	$18,553	$7,539
Other comprehensive income, net of tax:			
Foreign Currency:			
Foreign currency translation adjustments (includes $0, $(2) and $0 attributable to noncontrolling interest), net of taxes of $(45), $(78) and $48	**(75)**	(140)	87
Reclassification adjustment included in net income, net of taxes of $224, $30 and $0	**416**	55	—
Available-for-sale securities:			
Net unrealized gains, net of taxes of $40, $137, and $64	**64**	257	118
Reclassification adjustment included in net income, net of taxes of $(10), $(42) and $(36)	**(16)**	(79)	(68)
Cash flow hedges:			
Net unrealized gains, net of taxes of $140, $286 and $154	**260**	525	283
Reclassification adjustment included in net income, net of taxes of $18, $16 and $15	**36**	30	28
Defined benefit postretirement plans:			
Net actuarial loss from equity method investees arising during period, net of taxes of $0, $0 and $(32)	**—**	—	(53)
Reclassification adjustment included in net income, net of taxes of $11, $7 and $0	**26**	11	—
Net prior service credit arising during period, net of taxes of $262, $1,695 and $1,378	**428**	2,765	2,249
Amortization of net prior service credit included in net income, net of taxes of $(588), $(480) and $(361)	**(959)**	(782)	(588)
Other comprehensive income	**180**	2,642	2,056
Total comprehensive income	**6,698**	21,195	9,595
Less: Total comprehensive income attributable to noncontrolling interest	**(294)**	(302)	(275)
Total Comprehensive Income Attributable to AT&T	**$6,404**	$20,893	$9,320

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Balance Sheets

Dollars in millions except per share amounts

	December 31,	
	2014	2013
Assets		
Current Assets		
Cash and cash equivalents	$ 8,603	$ 3,339
Accounts receivable – net of allowances for doubtful accounts of $454 and $483	14,527	12,918
Prepaid expenses	831	960
Deferred income taxes	1,142	1,199
Other current assets	6,925	4,780
Total current assets	32,028	23,196
Property, Plant and Equipment – Net	112,898	110,968
Goodwill	69,692	69,273
Licenses	60,824	56,433
Other Intangible Assets – Net	6,139	5,779
Investments in Equity Affiliates	250	3,860
Other Assets	10,998	8,278
Total Assets	$292,829	$277,787
Liabilities and Stockholders' Equity		
Current Liabilities		
Debt maturing within one year	$ 6,056	$ 5,498
Accounts payable and accrued liabilities	23,592	21,107
Advanced billings and customer deposits	4,105	4,212
Accrued taxes	1,091	1,774
Dividends payable	2,438	2,404
Total current liabilities	37,282	34,995
Long-Term Debt	76,011	69,290
Deferred Credits and Other Noncurrent Liabilities		
Deferred income taxes	37,544	36,308
Postemployment benefit obligation	37,079	29,946
Other noncurrent liabilities	17,989	15,766
Total deferred credits and other noncurrent liabilities	92,612	82,020
Stockholders' Equity		
Common stock ($1 par value, 14,000,000,000 authorized at December 31, 2014 and 2013: issued 6,495,231,088 at December 31, 2014 and 2013)	6,495	6,495
Additional paid-in capital	91,108	91,091
Retained earnings	27,736	31,141
Treasury stock (1,308,318,131 at December 31, 2014 and 1,268,914,913 at December 31, 2013, at cost)	(47,029)	(45,619)
Accumulated other comprehensive income	8,060	7,880
Noncontrolling interest	554	494
Total stockholders' equity	86,924	91,482
Total Liabilities and Stockholders' Equity	$292,829	$277,787

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Cash Flows

Dollars in millions

	2014	2013	2012
Operating Activities			
Net income	**$ 6,518**	$ 18,553	$ 7,539
Adjustments to reconcile net income to net cash provided by operating activities:			
Depreciation and amortization	**18,273**	18,395	18,143
Undistributed earnings from investments in equity affiliates	**(27)**	(324)	(615)
Provision for uncollectible accounts	**1,032**	954	1,117
Deferred income tax expense	**1,772**	6,242	1,747
Net gain from sale of investments, net of impairments	**(1,532)**	(492)	(19)
Actuarial loss (gain) on pension and postretirement benefits	**7,869**	(7,584)	9,994
Abandonment of network assets	**2,120**	—	—
Changes in operating assets and liabilities:			
Accounts receivable	**(2,651)**	(1,329)	(1,365)
Other current assets	**(962)**	412	1,017
Accounts payable and accrued liabilities	**2,412**	(152)	1,798
Retirement benefit funding	**(560)**	(209)	—
Other – net	**(2,926)**	330	(180)
Total adjustments	**24,820**	16,243	31,637
Net Cash Provided by Operating Activities	**31,338**	34,796	39,176
Investing Activities			
Construction and capital expenditures:			
Capital expenditures	**(21,199)**	(20,944)	(19,465)
Interest during construction	**(234)**	(284)	(263)
Acquisitions, net of cash acquired	**(3,141)**	(4,113)	(828)
Dispositions	**8,123**	1,923	812
(Purchases) sales of securities, net	**(1,890)**	—	65
Return of advances to and investments in equity affiliates	**4**	301	—
Other	**—**	(7)	(1)
Net Cash Used in Investing Activities	**(18,337)**	(23,124)	(19,680)
Financing Activities			
Net change in short-term borrowings with original maturities of three months or less	**(16)**	20	1
Issuance of other short-term borrowings	**—**	1,476	—
Repayment of other short-term borrowings	**—**	(1,476)	—
Issuance of long-term debt	**15,926**	12,040	13,486
Repayment of long-term debt	**(10,400)**	(7,698)	(8,733)
Issuance of other long-term financing obligations	**107**	4,796	—
Purchase of treasury stock	**(1,617)**	(13,028)	(12,752)
Issuance of treasury stock	**39**	114	477
Dividends paid	**(9,552)**	(9,696)	(10,241)
Other	**(2,224)**	251	89
Net Cash Used in Financing Activities	**(7,737)**	(13,201)	(17,673)
Net increase (decrease) in cash and cash equivalents	**5,264**	(1,529)	1,823
Cash and cash equivalents beginning of year	**3,339**	4,868	3,045
Cash and Cash Equivalents End of Year	**$ 8,603**	$ 3,339	$ 4,868

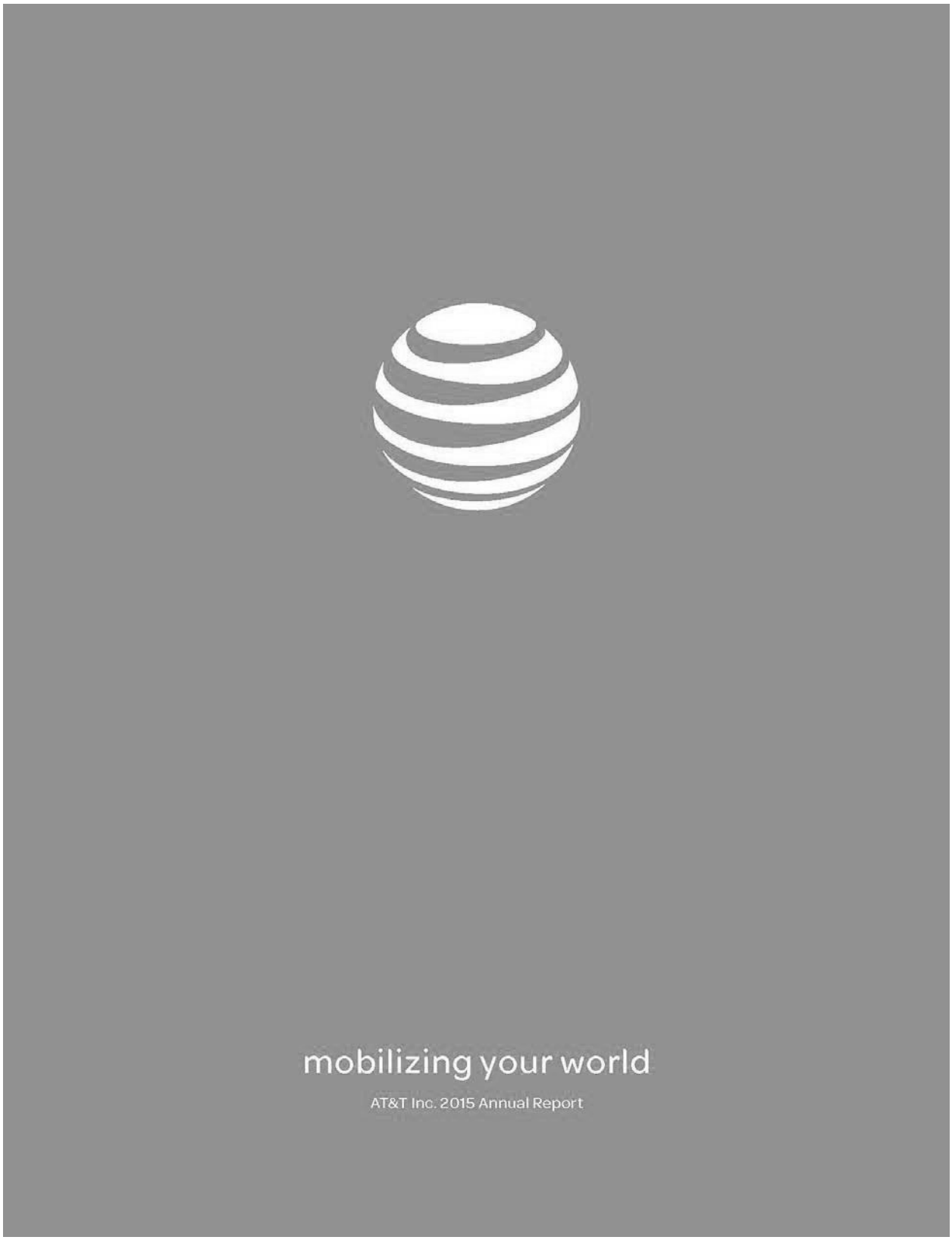
The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Changes in Stockholders' Equity

Dollars and shares in millions except per share amounts

	2014		2013		2012	
	Shares	Amount	Shares	Amount	Shares	Amount
Common Stock						
Balance at beginning of year	6,495	$ 6,495	6,495	$ 6,495	6,495	$ 6,495
Issuance of stock	—	—	—	—	—	—
Balance at end of year	6,495	$ 6,495	6,495	$ 6,495	6,495	$ 6,495
Additional Paid-In Capital						
Balance at beginning of year		$ 91,091		$ 91,038		$ 91,156
Issuance of treasury stock		4		(8)		120
Share-based payments		47		62		(78)
Share of equity method investee capital transactions		—		—		(160)
Change related to acquisition of interests held by noncontrolling owners		(34)		(1)		—
Balance at end of year		$ 91,108		$ 91,091		$ 91,038
Retained Earnings						
Balance at beginning of year		$ 31,141		$ 22,481		$ 25,453
Net income attributable to AT&T ($1.19, $3.39 and $1.25 per diluted share)		6,224		18,249		7,264
Dividends to stockholders ($1.85, $1.81 and $1.77 per share)		(9,629)		(9,589)		(10,236)
Balance at end of year		$ 27,736		$ 31,141		$ 22,481
Treasury Stock						
Balance at beginning of year	(1,269)	$(45,619)	(914)	$(32,888)	(568)	$ (20,750)
Repurchase of common stock	(48)	(1,617)	(366)	(13,028)	(371)	(12,752)
Issuance of treasury stock	9	207	11	297	25	614
Balance at end of year	(1,308)	$(47,029)	(1,269)	$(45,619)	(914)	$ (32,888)
Accumulated Other Comprehensive Income Attributable to AT&T, net of tax:						
Balance at beginning of year		$ 7,880		$ 5,236		$ 3,180
Other comprehensive income attributable to AT&T		180		2,644		2,056
Balance at end of year		$ 8,060		$ 7,880		$ 5,236
Noncontrolling Interest:						
Balance at beginning of year		$ 494		$ 333		$ 263
Net income attributable to noncontrolling interest		294		304		275
Distributions		(233)		(231)		(205)
Contributions		—		51		—
Acquisitions of noncontrolling interests		69		44		—
Acquisition of interests held by noncontrolling owners		(70)		(5)		—
Translation adjustments attributable to noncontrolling interest, net of taxes		—		(2)		—
Balance at end of year		$ 554		$ 494		$ 333
Total Stockholders' Equity at beginning of year		$ 91,482		$ 92,695		$105,797
Total Stockholders' Equity at end of year		$ 86,924		$ 91,482		$ 92,695

The accompanying notes are an integral part of the consolidated financial statements.


mobilizing your world
AT&T Inc. 2015 Annual Report

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of AT&T Inc.

We have audited AT&T Inc.'s (the Company) internal control over financial reporting as of December 31, 2015, based on criteria established in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework) (the COSO criteria). The Company's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Report of Management. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

As indicated in the accompanying Report of Management, management's assessment of and conclusion on the effectiveness of internal control over financial reporting did not include the internal controls of its DIRECTV and Mexico wireless businesses, which are included in the December 31, 2015 consolidated financial statements of the Company. DIRECTV constituted 20.3% of total assets and 9.9% of total revenues for the year then ended. The Mexico wireless businesses constituted 1.6% of total assets and 1.3% of total revenues for the year then ended. Our audit of internal control over financial reporting of the Company did not include an evaluation of the internal control over financial reporting of DIRECTV or the Mexico wireless businesses.

In our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of December 31, 2015, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of the Company as of December 31, 2015 and 2014, and the related consolidated statements of income, comprehensive income, changes in stockholders' equity and cash flows for each of the three years in the period ended December 31, 2015 and our report dated February 18, 2016 expressed an unqualified opinion thereon.

Dallas, Texas
February 18, 2016

Ernst & Young LLP

Report of Independent Registered Public Accounting Firm on Internal Control over Financial Reporting

The Board of Directors and Stockholders of AT&T Inc.

We have audited AT&T Inc.'s (the Company) internal control over financial reporting as of December 31, 2013, based on criteria established in Internal Control—Integrated Framework (1992 framework) issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). The Company's management is responsible for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting included in the accompanying Report of Management. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of December 31, 2013, based on the COSO criteria.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the consolidated balance sheets of the Company as of December 31, 2013 and 2012, and the related consolidated statements of income and comprehensive income, changes in stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2013 and our report dated February 21, 2014 expressed an unqualified opinion thereon.

Ernst & Young LLP

Dallas, Texas
February 21, 2014

Consolidated Statements of Income

Dollars in millions except per share amounts

	2015	2014	2013
		As Adjusted	
Operating Revenues			
Service	**$131,677**	$118,437	$119,252
Equipment	**15,124**	14,010	9,500
Total operating revenues	**146,801**	132,447	128,752
Operating Expenses			
Cost of services and sales			
Equipment	**19,268**	18,946	16,644
Broadcast, programming and operations	**11,996**	4,075	3,308
Other cost of services (exclusive of depreciation and amortization shown separately below)	**35,782**	37,124	31,239
Selling, general and administrative	**32,954**	39,697	28,414
Abandonment of network assets	**—**	2,120	—
Depreciation and amortization	**22,016**	18,273	18,395
Total operating expenses	**122,016**	120,235	98,000
Operating Income	**24,785**	12,212	30,752
Other Income (Expense)			
Interest expense	**(4,120)**	(3,613)	(3,940)
Equity in net income of affiliates	**79**	175	642
Other income (expense) – net	**(52)**	1,581	596
Total other income (expense)	**(4,093)**	(1,857)	(2,702)
Income Before Income Taxes	**20,692**	10,355	28,050
Income tax expense	**7,005**	3,619	9,328
Net Income	**13,687**	6,736	18,722
Less: Net Income Attributable to Noncontrolling Interest	**(342)**	(294)	(304)
Net Income Attributable to AT&T	**$ 13,345**	$ 6,442	$ 18,418
Basic Earnings Per Share Attributable to AT&T	**$ 2.37**	$ 1.24	$ 3.42
Diluted Earnings Per Share Attributable to AT&T	**$ 2.37**	$ 1.24	$ 3.42

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Comprehensive Income

Dollars in millions

	2015	2014	2013
			As Adjusted
Net income	**$13,687**	$6,736	$18,722
Other comprehensive income, net of tax:			
Foreign Currency:			
Translation adjustments (includes $(16), $0 and $(2) attributable to noncontrolling interest), net of taxes of $(595), $(45) and $(78)	**(1,188)**	(75)	(140)
Reclassification adjustment included in net income, net of taxes of $0, $224 and $30	**—**	416	55
Available-for-sale securities:			
Net unrealized gains, net of taxes of $0, $40, and $137	**—**	65	258
Reclassification adjustment included in net income, net of taxes of $(9), $(10) and $(42)	**(15)**	(16)	(79)
Cash flow hedges:			
Net unrealized (losses) gains, net of taxes of $(411), $140 and $286	**(763)**	260	525
Reclassification adjustment included in net income, net of taxes of $20, $18 and $16	**38**	36	30
Defined benefit postretirement plans:			
Amortization of net prior service credit included in net income, net of taxes of $(523), $(588) and $(480)	**(860)**	(959)	(782)
Net prior service credit arising during period, net of taxes of $27, $262 and $1,695	**45**	428	2,765
Reclassification adjustment included in net income, net of taxes of $0, $11 and $7	**—**	26	11
Other comprehensive income (loss)	**(2,743)**	181	2,643
Total comprehensive income	**10,944**	6,917	21,365
Less: Total comprehensive income attributable to noncontrolling interest	**(326)**	(294)	(302)
Total Comprehensive Income Attributable to AT&T	**$10,618**	$6,623	$21,063

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Balance Sheets
Dollars in millions except per share amounts

	December 31,	
	2015	2014
		As Adjusted
Assets		
Current Assets		
Cash and cash equivalents	$ 5,121	$ 8,603
Accounts receivable – net of allowances for doubtful accounts of $704 and $454	16,532	14,527
Prepaid expenses	1,072	831
Other current assets	13,267	9,645
Total current assets	35,992	33,606
Property, Plant and Equipment – Net	124,450	112,898
Goodwill	104,568	69,692
Licenses	93,093	60,824
Customer Lists and Relationships – Net	18,208	812
Other Intangible Assets – Net	9,409	5,327
Investments in Equity Affiliates	1,606	250
Other Assets	15,346	13,425
Total Assets	$402,672	$296,834
Liabilities and Stockholders' Equity		
Current Liabilities		
Debt maturing within one year	$ 7,636	$ 6,056
Accounts payable and accrued liabilities	30,372	23,592
Advanced billings and customer deposits	4,682	4,105
Accrued taxes	2,176	1,091
Dividends payable	2,950	2,438
Total current liabilities	47,816	37,282
Long-Term Debt	118,515	75,778
Deferred Credits and Other Noncurrent Liabilities		
Deferred income taxes	56,181	38,436
Postemployment benefit obligation	34,262	37,079
Other noncurrent liabilities	22,258	17,989
Total deferred credits and other noncurrent liabilities	112,701	93,504
Stockholders' Equity		
Common stock ($1 par value, 14,000,000,000 authorized at December 31, 2015 and 2014: issued 6,495,231,088 at December 31, 2015 and 2014)	6,495	6,495
Additional paid-in capital	89,763	91,108
Retained earnings	33,671	31,081
Treasury stock (350,291,239 at December 31, 2015 and 1,308,318,131 at December 31, 2014, at cost)	(12,592)	(47,029)
Accumulated other comprehensive income	5,334	8,061
Noncontrolling interest	969	554
Total stockholders' equity	123,640	90,270
Total Liabilities and Stockholders' Equity	$402,672	$296,834

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Cash Flows

Dollars in millions

	2015	2014	2013
		As Adjusted	
Operating Activities			
Net income	**$ 13,687**	$ 6,736	$ 18,722
Adjustments to reconcile net income to net cash provided by operating activities:			
Depreciation and amortization	**22,016**	18,273	18,395
Undistributed earnings from investments in equity affiliates	**(49)**	(27)	(324)
Provision for uncollectible accounts	**1,416**	1,032	954
Deferred income tax expense	**4,117**	1,948	6,345
Net loss (gain) from sale of investments, net of impairments	**91**	(1,461)	(492)
Actuarial (gain) loss on pension and postretirement benefits	**(2,152)**	7,869	(7,584)
Abandonment of network assets	**—**	2,120	—
Changes in operating assets and liabilities:			
Accounts receivable	**(535)**	(2,651)	(1,329)
Other current assets	**(1,789)**	(974)	445
Accounts payable and accrued liabilities	**1,291**	2,412	(152)
Retirement benefit funding	**(735)**	(560)	(209)
Other – net	**(1,478)**	(3,379)	25
Total adjustments	**22,193**	24,602	16,074
Net Cash Provided by Operating Activities	**35,880**	31,338	34,796
Investing Activities			
Construction and capital expenditures:			
Capital expenditures	**(19,218)**	(21,199)	(20,944)
Interest during construction	**(797)**	(234)	(284)
Acquisitions, net of cash acquired	**(30,759)**	(3,141)	(4,113)
Dispositions	**83**	8,123	1,923
Sales (purchases) of securities, net	**1,545**	(1,890)	—
Return of advances to and investments in equity affiliates	**1**	4	301
Other	**1**	—	(7)
Net Cash Used in Investing Activities	**(49,144)**	(18,337)	(23,124)
Financing Activities			
Net change in short-term borrowings with original maturities of three months or less	**(1)**	(16)	20
Issuance of other short-term borrowings	**—**	—	1,476
Repayment of other short-term borrowings	**—**	—	(1,476)
Issuance of long-term debt	**33,969**	15,926	12,040
Repayment of long-term debt	**(10,042)**	(10,400)	(7,698)
Issuance of other long-term financing obligations	**—**	107	4,796
Purchase of treasury stock	**(269)**	(1,617)	(13,028)
Issuance of treasury stock	**143**	39	114
Dividends paid	**(10,200)**	(9,552)	(9,696)
Other	**(3,818)**	(2,224)	251
Net Cash Provided by (Used in) Financing Activities	**9,782**	(7,737)	(13,201)
Net (decrease) increase in cash and cash equivalents	**(3,482)**	5,264	(1,529)
Cash and cash equivalents beginning of year	**8,603**	3,339	4,868
Cash and Cash Equivalents End of Year	**$ 5,121**	$ 8,603	$ 3,339

The accompanying notes are an integral part of the consolidated financial statements.

Consolidated Statements of Changes in Stockholders' Equity

Dollars and shares in millions except per share amounts

	2015		2014		2013	
	Shares	Amount	Shares	Amount	Shares	Amount
				As Adjusted		
Common Stock						
Balance at beginning of year	**6,495**	**$ 6,495**	6,495	$ 6,495	6,495	$ 6,495
Issuance of stock	**—**	**—**	—	—	—	—
Balance at end of year	**6,495**	**$ 6,495**	6,495	$ 6,495	6,495	$ 6,495
Additional Paid-In Capital						
Balance at beginning of year		**$ 91,108**		$ 91,091		$ 91,038
Issuance of treasury stock		**(1,597)**		4		(8)
Share-based payments		**252**		47		62
Change related to acquisition of interests held by noncontrolling owners		**—**		(34)		(1)
Balance at end of year		**$ 89,763**		$ 91,108		$ 91,091
Retained Earnings						
Balance at beginning of year		**$ 31,081**		$ 34,269		$ 25,440
Net income attributable to AT&T ($2.37, $1.24 and $3.42 per diluted share)		**13,345**		6,442		18,418
Dividends to stockholders ($1.89, $1.85 and $1.81 per share)		**(10,755)**		(9,630)		(9,589)
Balance at end of year		**$ 33,671**		$ 31,081		$ 34,269
Treasury Stock						
Balance at beginning of year	**(1,308)**	**$ (47,029)**	(1,269)	$(45,619)	(914)	$(32,888)
Repurchase of common stock	**(8)**	**(278)**	(48)	(1,617)	(366)	(13,028)
Issuance of treasury stock	**966**	**34,715**	9	207	11	297
Balance at end of year	**(350)**	**$ (12,592)**	(1,308)	$(47,029)	(1,269)	$(45,619)
Accumulated Other Comprehensive Income Attributable to AT&T, net of tax:						
Balance at beginning of year		**$ 8,061**		$ 7,880		$ 5,235
Other comprehensive income (loss) attributable to AT&T		**(2,727)**		181		2,645
Balance at end of year		**$ 5,334**		$ 8,061		$ 7,880
Noncontrolling Interest:						
Balance at beginning of year		**$ 554**		$ 494		$ 333
Net income attributable to noncontrolling interest		**342**		294		304
Distributions		**(294)**		(233)		(231)
Contributions		**—**		—		51
Acquisitions of noncontrolling interests		**383**		69		44
Acquisition of interests held by noncontrolling owners		**—**		(70)		(5)
Translation adjustments attributable to noncontrolling interest, net of taxes		**(16)**		—		(2)
Balance at end of year		**$ 969**		$ 554		$ 494
Total Stockholders' Equity at beginning of year		**$ 90,270**		$ 94,610		$ 95,653
Total Stockholders' Equity at end of year		**$123,640**		$ 90,270		$ 94,610

The accompanying notes are an integral part of the consolidated financial statements.

Exhibit Z: Schedule 16.1 Fees

File submitted separately as Vol III Exhibit Z-Schedule 16.1 Fees_Final_20161027.docx

Exhibit AA: Exhibit 16.1-1 Resource Unit Price Summary

File submitted separately as Vol III Exhibit AA-Exhibit 16.1-1 Resource Unit Price Summary_Final_20161027.docx

Exhibit CC: Exhibit 16.1-2 Resource Unit Price Decomposition

File submitted separately as Vol III Exhibit CC-Exhibit 16.1-2 Resource Unit Price Decomposition_Final_20161027.xlsx

Exhibit DD: Exhibit 16.1-3 Maximum Annual Fee

File submitted separately as Vol III Exhibit DD-Exhibit 16.1-3 Maximum Annual Fee_Final_20161027.docx

Exhibit FF: Exhibit 16.1-5 Firm Fixed Price for Applications M&O

Three files submitted separately as:

- Vol III Exhibit FF-Exhibit 16.1-5 Firm Fixed Price for Apps M and O_County_Final_20161027.xlsx
- Vol III Exhibit FF-Exhibit 16.1-5 Firm Fixed Price for Apps M and O_Department_Final_20161027.xlsx
- Vol III Exhibit FF-Exhibit 16.1-5 Firm Fixed Price for Apps M and O_Group_Final_20161027.xlsx

Exhibit GG: Exhibit 16.1-5b Firm Fixed Price for Applications M&O

File submitted separately as Vol III Exhibit GG-Exhibit 16.1-5b Firm Fixed Price for App M and O_Final_20161027.docx

Schedule 2.1 — Transition Plan

Table of Contents

1. Overview 4
2. Requirements 4
2.1. Human Resources Transition 4
2.2. Knowledge Transfer 4
2.3. Asset Transfer 5
2.4. Assignment or Management of Third Party Contracts/Licenses/Leases 5
2.5. Data Transfer 5
2.6. Compliance with Service Levels 5
2.7. Assumption of Current Projects 6
2.8. Communications/Governance Plan for the County and the Legacy Provider 6
2.9. Contingency Planning/Risk Mitigation 6
2.10. Measurable Success Criteria 6
2.11. Transition Project Plan 7
2.12. Transition Staffing 7
2.13. Transition Schedule 7
3. Transition Projects 8
3.1. Cross Functional Services 8
3.2. E-Mail Services 9
3.3. Development and Test Environment 10
3.4. Consolidated and Single Data Center 11
3.5. Storage Architecture 12
3.6. Service Portal 13
4. High-Level Transition Milestones and Tasks 14
4.1. Transition Start-up and Organization 14
4.2. Service Desk Framework 15
4.3. Application Services Framework 16

4.4. End-User Services Framework 18

4.5. Network Services Framework 19

4.6. Data Center Service Framework 21

4.7. Cross Functional Service Framework 23

5. Final Transition Milestones 25

1. OVERVIEW

Transition is the expeditious, seamless and uninterrupted changeover of Services within the scope described in this Request for Proposal (RFP) from the Legacy Provider to the Contractor.

Such transition shall be planned and accomplished by the Contractor in such a way as to have no adverse effect upon the County, nor upon the quality or continuity of the Services being provided.

The Contractor shall work in close cooperation with the Legacy Provider throughout the transition. From the start of the transition and prior to the final cutover date on which the Contractor will assume full responsibility for the Services, the Contractor shall "shadow" the Legacy Provider. This ensures a complete knowledge transfer of all information needed in providing the Services to the Contractor.

The Contractor shall develop and deliver a complete Transition Project Plan that will address all the requirements in Schedule 2.1 and fully implement the Services.

2. REQUIREMENTS

2.1. Human Resources Transition

For purposes of knowledge transfer or other reasons, it may be beneficial for the Contractor (or its subcontractors) to hire some of the personnel providing Services who are currently employed by the Legacy Provider (or by such Legacy Provider's subcontractors). The Contractor shall propose a process and communications strategy for soliciting, making offers to, and hiring such personnel.

2.2. Knowledge Transfer

Contractor shall propose and implement a complete and effective set of transition procedures that will ensure a complete and robust transfer of knowledge of County-specific functions, applications, designs, documentation, processes and any other data needed to provide current Services from the County and the Legacy Provider.

2.3. Asset Transfer

The County has a right to purchase from the Legacy Provider the assets that are currently used to provide the Services. The Contractor shall, as part of its due diligence and response to the RFP, analyze the current Assets and make a proposal to the County as to whether the Contractor will use some or all of such Assets.

Notwithstanding the foregoing, Contractor shall purchase from the Legacy Provider all Desktop Framework Assets (as that term is defined in the IT and Telecommunications Services Agreement dated January 24, 2006 and Restated on June 24, 2014 between the County of San Diego and HP Enterprise Services, LLC) at Contractor's Cutover to the End-User Services Framework. Contractor shall pay the Legacy Provider the net book value of the Desktop Framework Assets as determined by the terms of the IT and Telecommunications Services Agreement dated January 24, 2006 and Restated on June 24, 2014 between the County of San Diego and HP Enterprise Services, LLC. Contractor shall not be entitled to or claim from County any additional compensation for this purchase other than that allowed for in Schedule 16.1 – Fees.

2.4. Assignment or Management of Third-Party Contracts/Licenses/Leases

A number of Third-Party contracts, licenses and leases exist that are currently used to provide Services. The Contractor shall analyze this group of contracts, licenses and leases held by the Legacy Provider to determine which will transition to the Contractor. All County contracts, licenses and leases used to provide the Services currently, shall be transitioned to the Contractor. The Contractor shall propose and implement appropriate processes to assure the smooth transition of these contracts from the County and the Legacy Provider.

2.5. Data Transfer

The Contractor shall propose processes and techniques for transferring stewardship of County data from the Legacy Provider to the Contractor without compromising, disclosing, corrupting or losing such data.

2.6. Compliance with Service Levels

The Contractor shall develop a plan specifying firm dates by which Services transitioned will be expected to perform in full accordance to the Service Levels. Contractor and/or Legacy Provider shall maintain all Service Levels throughout the transition.

2.7. Assumption of Current Projects

A number of IT projects will be in various stages of completion when the Contractor transitions the Services. The Contractor shall assume control of all these projects without causing any material adverse impact to their individual deadlines, budgets and milestones.

2.8. Communications/Governance Plan for the County and the Legacy Provider

The Contractor and the Legacy Provider shall communicate and manage transition tasks and issues as they occur. The Contractor shall propose communications and governance strategies and plans to make the transition work smoothly with all the parties involved.

2.9. Contingency Planning/Risk Mitigation

The Contractor shall propose contingency planning and risk mitigation strategies to ensure the transition process shall not adversely affect the quality of the Services received by the County and its constituents.

2.10. Measurable Success Criteria

The County must have a clear understanding and accounting of when elements of the transition, particularly the cutover to the Contractor of a Service Framework, are accomplished successfully.

For each Service Framework, the Contractor shall propose an appropriate process (including measurable success criteria) by which the County can determine that the transition has been successfully completed, including a process by which not only the County, but also the Legacy Provider have the right to indicate as to whether the Services have been transitioned completely from the Legacy Provider to the Contractor. The County expects the Contractor to propose a staggered transition of the services, on a Service Framework by Service Framework basis, in the following order: (1) Service Desk, (2) Applications Services, (3) End User Services, (4) Network Services, and (5) Data Center Services. The only remaining Service Framework—Cross Functional Services—is integrated into each Service Framework and by its nature should ramp up incrementally throughout transition to correspond with the Cross Functional Services performed under each of the transitioned Service Frameworks. Because of such integration, upon the successful transition of each of the other Service Frameworks, the Cross Functional Services Framework should be completely transitioned to the Contractor.

2.11. Transition Project Plan

Contractor shall provide a detailed transition project plan and methodology, incorporating the elements described above and the projects, tasks and milestones defined below, as well as any assumptions made by the Contractor in the development of the transition plan.

2.12. Transition Staffing

Contractor shall assign, with County approval, a dedicated Transition Project Manager and dedicated Transition staff from the start to completion of the Transition of Services. Contractor Transition Project Manager shall provide weekly status reports on the progress of the Transition to the County.

2.13. Transition Schedule

Contractor shall complete the transition of Services by April 30, 2018. The transition starting date is the January 2, 2017. The tentative schedule for transition of the Service Frameworks is outlined below.

Task	Start Date	Completion Date
Transition Project Organization	1/2/2017	9/29/17
Transition Start-Up	1/2/2017	1/17/17
Service Desk Services	1/2/2017	4/30/18
Applications Services	1/2/2017	6/30/17
End-User Services	1/2/2017	7/31/17
Network Services	1/2/2017	8/31/17
Data Center Services	1/2/2017	4/30/18
Cross Functional Services	1/2/2017	4/30/18

3. TRANSITION PROJECTS

During the RFP and negotiation process with the Contractor, the County expects the Contractor to address the following key projects pertaining to transition:

3.1. Cross Functional Services

Cross Functional Services are a critical Component in the support and management of the Services. As each Cross Functional Component is developed and delivered, it should be documented completely, reviewed and approved by the County, and posted on the Service Portal. This document set will be referred to as the management plan.

Each Cross Functional Component will have a management plan. The basic outline for the management plan is: Introduction, Scope, Requirements, Design, Process and Appendixes to complete the document.

The initial transition of Cross Functional Services will require the completion and County approval of each management plan, respectively. The Contractor shall annually update the Cross Functional management plan and deliver to the County for approval. The Contractor shall maintain the content accuracy of the Service Portal for each Cross Functional Management plan.

The current Components of Cross Functional required to have a management plan are listed below:

1. Contract and Acquisition Management Services
2. Integrated Asset Management Services
3. Billing Management Services
4. Security Management Services
5. Service Delivery Management (SDM) Services
6. Architecture Services
7. Project Management Services
8. Integration and Testing Services
9. Incident Management Services
10. Problem Management Services
11. Change Management Services
12. Release Management Services
13. Configuration Management Services

14. Capacity Planning and Performance Management Services
15. Disaster Recovery Management Services
16. Identity Access Management Services
17. Reporting Management Services
18. Domain Name Management Services
19. Business Analyst Services

3.2. E-Mail Services

The County of San Diego E-Mail system, based on Microsoft Exchange 2010, requires an upgrade that shall be performed at the time of Transition. As E-Mail is a critical service used by all County, the technical currency and operational reliably must be sustained. Additional features and functions of the E-Mail service, not currently in place, shall be enabled to facilitate current and future County business requirements.

The current Exchange 2010 data center hosted service is operationally reliable but not technically current. The current service does not provide features and functions needed for County use, such as archive, e-journaling or e-discovery. County E-mail uses a retention cycle of no more than 60 days for any message in the current environment. This stated retention cycle will remain in place without exception. Spam and Malware protection is offered through a data center hosted service using Cisco IronPort. With respect to licensing, the County has a Microsoft Enterprise Agreement (EA) in place that includes Office 365. The Microsoft EA also includes licensing for the data center Exchange servers.

The next generation E-Mail system for County users should put into place technical currency coupled with needed features. Always-on and Always-available are earmarks to the new and updated service. Options to move to cloud based should be considered as well as potential hybrid type solutions.

Contractor shall develop and deliver an E-Mail transition plan for County approval. The E-Mail transition plan shall include the migration strategy, the overall design of E-Mail, communications package, detailed tasks and schedules and other associated project planning information. The implementation of the E-Mail transition plan shall occur during the transition of Services. The initial list of items that are in scope are outlined below:

- Migrate to the current version of Exchange
- Migrate to the current version of Outlook to desktops

- Maintain County retention policies without exception
- Complete migration of all active E-Mail users
- Maintain versions of Exchange within 12 months of new releases
- Maintain patch levels of Exchange within 3 months of any new release
- Unlimited Mailbox storage
- Unlimited user archive storage
- Immutably preserve or In-Place Hold for user data, as requested
- Redundancy built-in to insure minimal down time for E-Mail user
- Continuous backup to prevent failure due to data loss
- Malware and anti-spam protection at the perimeter and within the Outlook client
- Protection against unsafe attachments at the perimeter and the Outlook client
- Data Loss Prevention implemented per County policy
- E-discovery implemented and used as requested by the County
- Migration of PST files to Exchange archive
- Elimination of PST file from End-User environment
- Implement Outlook Web Access (OWA)
- Lockdown OWA to further protect County information
- Mobile aware and productivity included

3.3. Development and Test Environment

The County requires a robust, scalable, and dynamic, virtual-based Development and Test Environment. This enhanced capability will bring the provisioning of standard servers and storage from preconfigured templates within hours with a near replicated production environment. This ability will reduce cost, delays in project schedules and increase customer satisfaction.

The Development and Test Environment shall have resource management tools to track usage for cost management through the agreed upon method of billing. As an agile virtual environment that may reside in the data center, private cloud or hybrid combination this represents an optimized infrastructure built to perform work on-demand. The need to deploy dedicated physical servers hosted in the data center for Development and Test requirements should be eliminated. The process of adding a physical server to support Development and Test will follow the County exception to standards process.

Contractor shall develop and deliver a Development and Test transition plan for County approval. The Development and Test transition plan shall include the migration strategy, the overall design of the Development and Test environment, communications package, operational procedures, detailed tasks and schedules and other associated project planning information. The implementation of the Development and Test transition plan shall occur during the transition of Services. The initial list of items that are in scope are outlined below:

- Comply with Schedule 4.3, Operational Services, section 6.9 Development and Test Services
- Design based on data center, private cloud or hybrid combination approach
- Ability to stage unused instances only consuming storage
- Provision required environment within hours
- Scalable to support County Application Development demands
- Architected to support efficient and cost effective license models
- Detailed daily usage report by server
- Ability to provision a standard set of database, application ready, and web servers
- Meet to all associated Service Levels
- Ability to provision standard server types (e.g. web server, application server and database server)

3.4. Consolidated and Single Data Center

The County currently operates two production data centers. The initial plan was that the second data center would act as a disaster recovery site for the other and vice versa. As data center methodologies have emerged the need to operate two unique production data centers may not be warranted.

Leveraging changes being proposed in the Disaster Recovery Services section, it seems feasible that the County can consolidate to a single production data center. The reduction in physical computing assets along with the reductions in redundant and duplicative license costs and simplified application architecture make the feasibility of consolidating desirable.

Contractor shall develop and deliver a consolidated data center transition plan for County approval. The consolidated data center transition plan shall include the migration strategy, the overall design of consolidated data center environment, communications package, operational procedures and processes, detailed tasks and schedules and other associated project planning information. The implementation of the consolidated transition plan shall occur during the transition of Services. The initial list of items that are in scope are outlined below:

- Compliance with Schedule 4.3, Operational Services
- Network architecture design
- Storage architecture design
- Virtual server farm design
- Internet connection
- Hybrid cloud design
- Migration sequence of servers
- License consolidation
- Server/application consolidation
- Multiple and redundant WAN connections to County Points of Presence sites

3.5. Storage Architecture

The County of San Diego Storage Architecture is used to host End-User unstructured data and Portfolio Application data. The current storage architecture does not provide functions and features needed to manage and control the constant increases to physical data requirements. Appropriate tier of storage based on specific data types along with archiving techniques to migrate old and unused data to lower cost storage solutions can provide needed features of the storage architecture.

County Portfolio Application data requires a storage architecture that facilitates a higher degree of optimization. Portfolio application data repositories are not archived or use tier methodology which increases data bloat and decreases overall application performance. Strategies in Portfolio Application data management are a requirement for the storage architecture delivered in Transition.

The development of cloud based storage alternatives provides features that can enhance End-User productivity are not in place. Allowing remote or mobile End-Users the ability to have data available at all times, allow data synchronization, security of data, single cloud storage option and facilitate End-User device backups are needed requirements of the managed storage architecture.

Emerging methodologies of storage in the data center are evolving. Storage architectures range from traditional storage models, to virtual storage solutions to more advanced hyper-converged infrastructure. Hybrid and cloud based storage solutions exist that further enhance an overall architecture for storage. The

Contractor shall be required to develop a storage architecture and strategy that will manage County data well into the future.

Contractor shall develop and deliver a storage architecture transition plan for County approval. The storage architecture transition plan shall include the migration strategy of current data repositories, the overall design of storage environment, a cloud based strategy for End-Users, communications package, operational procedures and processes, detailed tasks and schedules and other associated project planning information. The implementation of the storage architecture transition plan shall occur during the transition of Services. The initial list of items that are in scope are outlined below:

- Comply with Schedule 4.3, Operational Services, section 6, Data Center Services
- Design a storage architecture for Portfolio Applications that uses more advanced techniques
- Design an End-User storage architecture for unstructured data in both data center centric and cloud based environments
- Support a highly virtual infrastructure in the storage architecture
- Develop archiving of data that meets certain criteria
- Develop and implement multiple tiers of storage based on data classifications
- Backup and recovery techniques that assure zero data lost for critical County data
- Backup and recovery techniques that assure near zero data lost for non-critical County data
- End-User reporting and data management capabilities via the Service Portal
- Centralized management of all data repositories by Contractor
- Scalable storage infrastructure that immediately meets critical demands
- Access speed

3.6. Service Portal

The need for a centralized and continuously managed focal point for all communications and information related to the Services is the fundamental requirement of the Service Portal. The Service Portal can provide enterprise wide communications and information assisting End-Users in resolving Incidents on their own as well as providing user tips and FAQs on the Services. The Service Portal shall be the main communication and information hub to all End-Users from the Contractor.

Contractor shall develop and deliver a Service Portal transition plan for County approval. The Service Portal transition plan shall include the migration strategy of current repositories, the overall design of Service

Portal environment, communications package, operational procedures and processes, detailed tasks and schedules and other associated project planning information. The implementation of the Service Portal transition plan shall occur during the transition of Services. The initial list of items that are in scope are outlined below:

- Comply with Schedule 4.3, Operational Services
- Design access to the Service Portal from the internet and the County intranet
- Create and submit Incidents and Services Requests
- View a list of all Incidents and Services Requests
- Allow End-Users to change and reset passwords
- View an up-to-date knowledge base with solutions, tip sheets and Frequently asked Questions (FAQs)
- View Countywide announcements related to the Services
- Access all Contractor deliverables and reports
- Service Request Management Services landing page
- Access to the Standards and Procedures Manual
- Help desk tip sheets, FAQs and end user self-help (self-service portal) information
- Service Levels Reports
- Management Plans
- RCA and Reports Portal
- SSO integration
- Post all published IT related material

4. HIGH-LEVEL TRANSITION MILESTONES AND TASKS

4.1. Transition Start-up and Organization

Task	Due Date	Transition Milestone
1. Each party shall assemble and name a transition management team for each Service Framework, including overall transition managers responsible for oversight of the entire transition process for each party.	1/2/2017	
2. Deliver to the County a detailed process and communications strategy for soliciting, making	N/A	

Task	Due Date	Transition Milestone
offers to, and hiring personnel used to perform the services.		
3. Propose, finalize and implement the communications and governance plan for the County and the County's Legacy Provider.	1/13/2017	
4. Conduct kick-off meetings with the Legacy Provider's disentanglement teams and the County's transition teams.	1/17/2017	

4.2. Service Desk Framework

Task	Due Date	Transition Milestone
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	2/2/2017	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the	N/A	

Task	Due Date	Transition Milestone
services (including any applicable Cross-Functional Services) to the County under this Service Framework.		
7. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	1/18/2017	
9. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	3/28/2017	
10. Submit for County approval the design document for the Service Portal	2/23/2017	
11. Finalize and deliver the Service Portal. Add Service Desk related content to the Service Portal	3/28/2017	
12. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	04/30/18	Yes

4.3. Application Services Framework

Task	Due Date	Transition Milestone
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	

Task	Due Date	Transition Milestone
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	1/18/2017	
9. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	6/30/2017	

Task	Due Date	Transition Milestone
10. Add Applications Services related content to the Service Portal	6/30/2017	
11. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	6/30/2017	Yes

4.4. End-User Services Framework

Task	Due Date	Transition Milestone
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
5. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
6. Complete the assignment to the Contractor of third party contracts, licenses and leases that are	N/A	

Task	Due Date	Transition Milestone
currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.		
7. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
9. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	1/18/2017	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	7/31/2017	
11. Add End-User Services related content to the Service Portal	7/31/2017	
12. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	7/31/2017	Yes

4.5. Network Services Framework

Task	Due Date	Transition Milestone
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility	N/A	

Task	Due Date	Transition Milestone
of the Contractor as of the Cutover Date for this Service Framework.		
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under this Service Framework, as applicable) and make offers to same.	N/A	
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	1/18/2017	
9. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service	8/31/2017	

Task	Due Date	Transition Milestone
Framework), incorporating all of the County's suggestions and comments.		
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	8/31/2017	
11. Add Network Services related content to the Service Portal	8/31/2017	
12. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	8/31/2017	Yes

4.6. Data Center Service Framework

Task	Due Date	Transition Milestone
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under	N/A	

Task	Due Date	Transition Milestone
this Service Framework, as applicable) and make offers to same.		
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
9. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	1/18/2017	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	9/29/2017	
11. Add Data Center Services related content to the Service Portal	9/29/2017	
12. Submit for County approval the design document for the E-Mail Service	1/30/2017	
13. Submit for County approval the design document for the Development and Test Environment	2/13/2017	

Task	Due Date	Transition Milestone
14. Submit for County approval the design document for the Consolidated Data Center	4/25/2017	
15. Submit for County approval the design document for the Storage Architecture	1/20/2017	
16. Develop and Deliver E-Mail Services	4/26/2017	
17. Develop and Deliver Development and Test Environment	8/4/2017	
18. Develop and deliver Consolidated Data Center	9/29/2017	
19. Develop and deliver Storage Architecture	7/5/2017	
20. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	04/30/18	Yes

4.7. Cross Functional Service Framework

Task	Due Date	Transition Milestone
1. Identify the current projects pertaining to this Service Framework (including current projects for Cross-Functional Services applicable to this Service Framework) that will be the responsibility of the Contractor as of the Cutover Date for this Service Framework.	N/A	
2. Provide the County with a detailed disaster recovery plan for this Service Framework (as well as the Cross-Functional Services applicable to this Service Framework) for its review, comment and approval.	Cutover Date minus 90 days	
3. Shadow the Legacy Provider and implement knowledge transfer processes for this Service Framework and the Cross-Functional Services applicable to this Service Framework.	N/A	
4. Complete interviews of personnel providing services to the County under this Service Framework (including any personnel providing Cross-Functional Services to the County under	N/A	

Task	Due Date	Transition Milestone
this Service Framework, as applicable) and make offers to same.		
5. Complete the assignment to the Contractor of third party contracts, licenses and leases that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
6. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
7. Complete the assignment to the Contractor of assets that are currently used to provide the services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
8. Hire personnel providing services (including any applicable Cross-Functional Services) to the County under this Service Framework.	N/A	
9. Deliver a reasonable and appropriate draft Standards and Procedures Manual sections to the County pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework) for the County's review, comment and approval.	1/18/2017	
10. Finalize and deliver to the County the Standards and Procedures Manual sections pertaining to this Service Framework (including any Cross-Functional Services applicable to this Service Framework), incorporating all of the County's suggestions and comments.	9/29/2017	
11. Develop and deliver to the County for approval a completed Management Plan for each Cross Functional Component	9/29/2017	
12. Add all Cross Functional Services content to the Service Portal	9/29/2017	
13. Add all Cross Functional Management Plans to the Service Portal	9/29/2017	

Task	Due Date	Transition Milestone
14. Implement and deliver each Cross Functional Management Plan	9/29/2017	
15. Cutover Date for this Service Framework (including any Cross-Functional Services applicable to this Service Framework), effective date of the Service Levels applicable to this Service Framework, implementation date for the final approved Disaster Recovery Plan for this Service Framework.	04/30/2018	Yes

5. FINAL TRANSITION MILESTONES

Task	Due Date	Transition Milestone
1. Final date of any interim Service Levels	N/A	
2. Completion date of Cross Functional Services Transition Project	9/29/2017	
3. Completion date of E-Mail Services Transition Project	4/26/2017	
4. Completion date of Development and Test Environment Transition Project	8/4/2017	
5. Completion date of Consolidated data center Transition Project	9/29/2017	
6. Completion date of Storage Architecture Transition Project	7/5/2017	
7. Completion date of Service Portal Transition Project	3/28/2017	
8. Delivery date of first invoice covering all Services.	10/10/2017	
9. Provide a listing of Contractor Personnel to reside at various County Locations	10/2/2017	
10. Provide an update to Contractor Key Personnel	10/2/2017	
11. Final completion date for all transition activities	04/30/2018	Yes

END OF SCHEDULE

Schedule 2.2 – Termination Fees During Transition

TERMINATION FEES BY MONTH

MONTH	AMOUNT
1	$ 1,222,912
2	$ 2,485,663
3	$ 3,936,137
4	$ 5,585,573
5	$ 7,488,248
6	$ 9,279,999
7	$ 10,252,618
8	$ 11,163,589
9	$ 12,172,527

END OF SCHEDULE

Schedule 3.2 – Form Bill of Sale

The County of San Diego ("County") acting through its Chief Administrative Officer and Purchasing Agent, and Peraton Enterprise Solutions LLC ("Contractor"), a Limited Liability Company, are Parties to the Information Technology and Telecommunications Service Agreement dated as of November 15, 2016, (the "Agreement"), pursuant to which the County has agreed to convey, assign, transfer, and deliver to Contractor the Purchased Assets designated to be transferred from the County to Contractor, as set forth in Appendix A.5 (the "Purchased County Assets") (terms capitalized in this Bill of Sale but not defined herein shall have the meanings ascribed to them in the Agreement).

For [$_____] and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the County does hereby sell, transfer, assign, convey, and deliver to Contractor, its successors and assigns, in accordance with the Agreement, all right, title, and interest in and to the Purchased County Assets.

THE PURCHASED COUNTY ASSETS ARE DELIVERED TO CONTRACTOR "AS IS, WHERE IS" AND CONTRACTOR ACKNOWLEDGES THAT, EXCEPT AS EXPRESSLY SET FORTH IN THE AGREEMENT AND HEREIN, THE COUNTY HAS NOT MADE, DOES NOT MAKE, AND WILL NOT MAKE ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, ON WHICH CONTRACTOR HAS RELIED OR MAY RELY, WITH RESPECT TO THE MERCHANTABILITY, FITNESS, SAFETY, DESIGN, CONDITION, QUALITY, CAPACITY, OPERATION, PERFORMANCE, DURABILITY, OR SUITABILITY FOR CONTRACTOR'S PURPOSES OF THE PURCHASED COUNTY ASSETS IN ANY RESPECT, THE PURCHASED COUNTY ASSETS' COMPLIANCE WITH ANY LAW, RULE, SPECIFICATION, OR CONTRACT PERTAINING THERETO, OR PATENT STATUS, PATENTABILITY, PATENT INFRINGEMENT, VISIBLE OR LATENT DEFECTS, OR ANY OTHER REPRESENTATION, WARRANTY, OR COVENANT, EXPRESS OR IMPLIED.

Notwithstanding the foregoing, the County hereby assigns and conveys to Contractor the full benefit of all representations, warranties, and indemnities held or enjoyed by the County with respect to the Purchased County Assets, to the extent assignable by the grantor thereof.

The County agrees that it will, at Contractor's reasonable request, without further consideration, do, execute, acknowledge, and deliver or will cause to be done, executed, acknowledged, and delivered, all such further acts, deeds, assignments, transfers, or conveyances as may be considered by Contractor, its successors or assigns, to be reasonably necessary or proper for the sale, transfer, assignment, or conveyance of the Purchased County Assets.

This instrument shall be binding upon, inure to the benefit of, and be enforceable by, any of Contractor's successors and assigns.

The County has caused this Bill of Sale to be signed on its behalf by a duly authorized individual as of _____.

COUNTY OF SAN DIEGO

By: _____

Name: _____

Title: _____

Acknowledgement and Acceptance

Contractor hereby acknowledges and accepts the County's transfer of its entire right, title, and interest in and to the Purchased County Assets and has agreed and accepted the terms and conditions of this Bill of Sale by authorizing a signature on its behalf by a duly authorized individual as of _____.

Peraton Enterprise Solutions LLC

By: _____

Name: _____

Title: _____

END OF SCHEDULE

Schedule 3.3 – Form Assignment and Assumption Agreement

The County of San Diego ("County"), acting through its Chief Administrative Officer and Purchasing Agent, and Peraton Enterprise Solutions LLC ("Contractor"), a Limited Liability Company, are Parties to the Information Technology and Telecommunications Service Agreement dated as of November 15, 2016 (the "Agreement"), pursuant to which the County has agreed to convey, assign, transfer, and deliver to Contractor the Assigned Leases and the Assigned Contracts described in the Agreement (collectively, the "Assigned Assets"). The Agreement is incorporated by this reference, and terms capitalized in this Assignment and Assumption Agreement but not defined herein shall have the meanings ascribed to them in the Agreement.

For valuable consideration, the receipt of which is hereby acknowledged by the Parties, the County does hereby sell, transfer, assign, delegate, convey and deliver to Contractor, its successors and assigns, and Contractor hereby accepts and assumes, all right title, and interest in and to, and all obligations associated with, the Assigned Assets.

IT IS EXPRESSLY UNDERSTOOD THAT THE COUNTY MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE EQUIPMENT THAT IS THE SUBJECT OF THE ASSIGNED LEASES, ALL OF WHICH IS BEING ACCEPTED "AS IS."

The County agrees that it will, at Contractor's reasonable request, without further consideration, do, execute, acknowledge, and deliver or will cause to be done, executed, acknowledged, and delivered, all such further acts, deeds, assignments, transfers, or conveyances as may be considered by Contractor, its successors or assigns, to be reasonably necessary or proper for the sale, transfer, or conveyance of the Assigned Assets. This instrument shall be binding upon, inure to the benefit of, and be enforceable by, any Contractor's successors and assigns.

The Parties hereto have caused this Assignment and Assumption Agreement to be signed on their behalf by duly authorized individuals as of _____.

COUNTY OF SAN DIEGO	**PERATON ENTERPRISE SOLUTIONS LLC**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

END OF SCHEDULE

Schedule 4.3 — Operational Services

Table of Contents

1. Overview of Services 6
1.1. Overview 6
1.2. High Level Requirements 6
1.3. Environment 7
1.4. Service Requirements 9
2. Cross Functional Services 12
2.1. Overview 12
2.2. High Level Requirements 13
2.3. Contract and Acquisition Management Services 14
2.4. Integrated Asset Management Services 19
2.5. Billing Management Services 24
2.6. Security Management Services 27
2.7. Service Delivery Management (SDM) Services 36
2.8. [Reserved] 40
2.9. Project Management Services 40
2.10. Integration and Testing Services 43
2.11. Incident Management Services 46
2.12. Problem Management Services 50
2.13. Change Management Services 55
2.14. Release Management Services 59
2.15. Configuration Management Services 63
2.16. Capacity Planning and Performance Management Services 68
2.17. Disaster Recovery Management Services 72
2.18. Identity Access Management Services 76
2.19. Reporting Management Services 81
2.20. Domain Name Management Services 85

2.21. Business Analyst Services 87
2.22. Chief Technical Architect (CTA) 89
2.23. Enterprise Application Architect (EAA) 92
2.24. Innovation Management Services 94
3. Service Desk Services 97
3.1. Overview 97
3.2. High Level Requirements 97
3.3. Environment 99
3.4. Roles and Responsibilities 99
3.5. Service Request Management Services 107
4. End-User Services 111
4.1. Overview 111
4.2. High Level Requirements 111
4.3. Environment 112
4.4. Roles and Responsibilities 113
4.5. Desktop Computing Services 120
4.6. Core Software Services 128
4.7. County Retained Assets Services 132
4.8. Mobile Device Support Services 135
4.9. Unified Communications Services 138
4.10. Catalog Services 141
4.11. Network Printer Services 145
4.12. Electronic File Sharing and Synchronization Services 148
4.13. Audio/Video (A/V) Conference Rooms Services 150
4.14. Digital Signage Services 151
4.15. Reserved. 153
4.16. Survey Solution Support Services 154

5. Network Services....156
5.1. Overview....156
5.2. High Level Requirements....157
5.3. Environment....159
5.4. Roles and Responsibilities....160
5.5. Data Network Services....163
5.6. Remote Access Services....168
5.7. Voice Services....172
5.8. Network Security Services....182
5.9. Video Conferencing Services....188
5.10. Video Streaming and Archiving Services....193
5.11. Mobility Infrastructure Services....196
5.12. Wireless Network Access Services....203
5.13. Third-Party Network Access Services....206
5.14. External DNS Management Services....211
5.15. IP Address Management Services....214
5.16. New Site Installation Services....217
5.17. Interactive Voice Services....220
5.18. Mobility Services....224
6. Data Center Services....227
6.1. Overview....227
6.2. High Level Requirements....227
6.3. Environment....229
6.4. Roles and Responsibilities....230
6.5. Security Services....234
6.6. Mainframe Services....238
6.7. Application Infrastructure Services....240

6.8. Infrastructure Services 252
6.9. Development and Test Services 259
6.10. E-Mail Services 263
6.11. Unified Communications Infrastructure Services 270
6.12. Storage Services 276
6.13. Backup and Recovery Services 284
6.14. Managed Print Services 287
6.15. Public Key Infrastructure (PKI) Services 289
7. Applications Services 293
7.1. Overview 293
7.2. Application Maintenance and Operations Services 293
7.3. Application Development Services 312
7.4. Electronic Health Records (EHR) Program Management Services 316

1. OVERVIEW OF SERVICES

1.1. Overview

This section describes the Services to be provided by the Contractor in various Service Frameworks, collectively also described herein as the Statement of Work (SOW). The objectives and requirements described in this Section 1 "Overview of Services" shall apply to all Service Frameworks without exception.

Capitalized terms used herein shall have the meaning assigned to them in Schedule A (Defined Terms) to the Agreement unless otherwise expressly defined in this Schedule.

1.2. High Level Requirements

1.2.1. Contractor shall provide Services to the County with a high level of quality and performance that meet or exceed the Service Levels.

1.2.2. Contractor shall provide equal or better service on all Service Frameworks in highest performance, capacity, and functionality as provided by the Legacy Provider.

1.2.3. Contractor shall provide continuous improvement to increase efficiency and effectiveness of County IT and Telecommunications Services over the life of the Agreement.

1.2.4. Contractor shall provide the technology expertise and resources required to provide Services in the most efficient and effective manner to meet the County's requirements.

1.2.5. Contractor shall provide strategies on emerging technologies that improve the County business operations and processes.

1.2.6. Contractor shall participate in, and support, the County's retained authorities in architecture, technology planning and standards establishment.

1.2.7. Contractor shall acquire and implement Services with availability guarantees that meet or exceed the defined Service Levels.

1.2.8. Contractor shall provide Services that can leverage operational scale and best practices to achieve optimum County price performance.

1.2.9. Contactor shall provide an annual report on improvements made since the previous report and improvements planned in the next year.

1.2.10. Contractor shall provide continuous improvement in Service Levels and provide a plan annually for improvements to Service Levels.

1.2.11. Contractor shall perform technology refresh and maintain technical currency that exceed or meet requirements.

1.2.12. Contractor shall acquire ongoing feedback mechanisms to ensure performance meets expectations.

1.2.13. Contractor shall maintain compliance with industry standards (e.g., ITIL) and government regulations.

1.2.14. Contractor shall maintain a customer focus and customer satisfaction while providing Services that are measurable and includes continuous improvement.

1.3. Environment

1.3.1. Tiers of Support

1.3.1.1. Contractor shall provide the up to five (5) tiers of support to End-Users.

1.3.1.2. Contractor shall provide all Tiers of Support 24/7/365.

1.3.1.3. Contractor shall continuously improve Tier 0 for End-User self-service.

1.3.1.4. Contractor shall continuously improve the performance and increase the knowledge at Tier 1 to resolve more End-Users Incidents at first call.

1.3.1.5. Defined Tiers of Support:

1.3.1.5.1. Tier 0

Tier 0 is the continuous updating and posting on the Service Portal of automated or self-service solutions, documents, instructions, videos, FAQs and like material that County End-Users can access without the aid of the Service Desk or Contractor Personnel.

1.3.1.5.2. Tier 1

Tier 1 are Service Desk calls that can provide basic support and troubleshooting, such as password resets, printer configurations, break-fix instructions, Incident routing and escalation to Tier 2 and Tier 3 support for End-Users. May also escalate to applications support or call for outside Third-Party maintenance (Tier 4), as needed.

1.3.1.5.3. Tier 2

Tier 2 support involves technical knowledge by more experienced technicians who have strong exposure to troubleshooting and handles break-fix, configuration issues, troubleshooting, software installations, and hardware. Tier 2 handles escalated Incidents from Tier 1. Tier 2 shall escalate unresolved Incidents to Tier 3 or to Tier 4.

1.3.1.5.4. Tier 3

Tier 3 is a very specialized job provided by the specialists who are usually involved in the product development and are capable of handling complex Incidents.

1.3.1.5.5. Tier 4

Tier 4 refers to Third-Party support, outside the County or Contractor. Escalation to Tier 4 support is for Incident resolution. This usually involves hardware and software Third-Party support for Portfolio Applications as an example.

1.3.2. Hardware and Software

Contractor shall provide all Hardware, Software, tools and knowledge databases used in the delivery of Services for each Service Framework. Contractor shall provision, install, manage, maintain, and support these Assets.

1.3.3. Facilities

1.3.3.1. County

All County Locations are within scope of the Agreement.

1.3.3.2. Contractor

All Locations utilized by the Contractor to provide the Services shall be provided, maintained, provisioned, and managed by the Contractor.

1.3.4. Personnel

Contractor shall be responsible for providing staff resources with the skills, qualifications, and experience to perform the Services in a high quality manner and to meet or exceed all Service Levels. Contractor's Account Executive, Contract Manager and two selected Key Personnel shall reside at the County Administration Center. A listing of Contractor Personnel to reside at various County Locations is to be developed and included in the final Transition Plan.

1.3.5. Policies, Procedures and Standards

Contractor shall be responsible for complying with all of the County's policies, procedures, and standards, including the Standards and Procedures Manual.

1.3.6. Agreements and Licenses

Contractor shall be responsible for the acquisition, management, and support of all agreements and licenses required for the Services.

1.3.7. Required Language(s)

English is the current required language. Contractor shall ensure that the level of English communications by all Contractor resources is sufficient to (i) be understandable by County staff and (ii) understand County staff.

1.4. Service Requirements

The descriptions of Operational Services in this Schedule follow the hierarchy of objectives and requirements:

1.4.1. This Overview of Services provides high-level requirements that apply to all of the Service Frameworks.

1.4.2. Each individual Service Framework includes a summary section describing requirements that apply to all of the Framework Components within the given Service Framework.

1.4.3. Each Framework Component includes requirements that apply specifically to the Framework Component, except for the Cross Functional Service Framework.

1.4.4. The Cross Functional Service Framework Components include requirements that apply to all Service Frameworks and Framework Components.

1.4.5. The Service Levels, referenced in Schedule 4.8, contain descriptions of Service Level requirements that apply across all the Service Frameworks.

1.4.6. Within each section, tables describing Roles and Responsibilities are included. These tables depict the County's Plan, Build, and Operate structure.

1.4.7. Service requirements in this Section use the structure depicted below:

Overview of Services

- Overview
- High Level Requirements
- Environment
- Service Requirements

These apply to all Service Frameworks and Framework Components

Service Frameworks

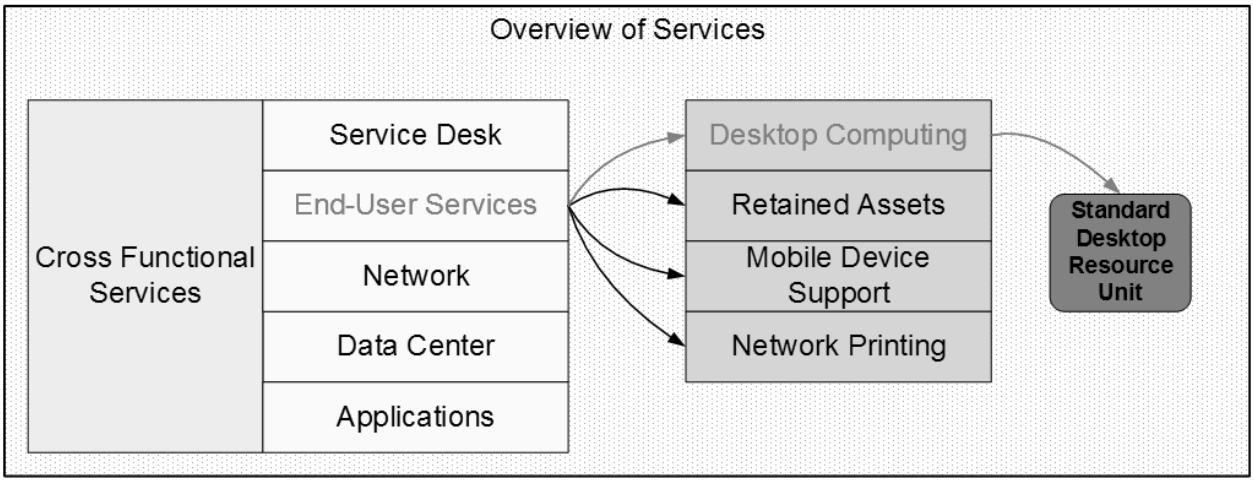
- Overview
- High Level Requirements
- Environment
- Roles and Responsibilities
  - Plan
  - Build
  - Operate

These apply to all the Framework Components within the specific Service Framework

Framework Components

- Overview
- High Level Requirements
- Environment
- Roles and Responsibilities
  - Plan
  - Build
  - Operate

These correspond to specific Resource Units



2. CROSS FUNCTIONAL SERVICES

2.1. Overview

This section pertains to the Cross Functional Services Framework. Cross Functional Services consist of the Plan, Build and Operate Services that spans across all Service Frameworks.

Cross Functional Services are composed of the following Framework Components:

- Contract and Acquisition Management Services
- Integrated Asset Management Services
- Billing Management Services
- Security Management Services
- Service Delivery Management (SDM) Services
- Architecture Services
- Project Management Services
- Integration and Testing Services
- Incident Management Services
- Problem Management Services
- Change Management Services
- Release Management Services
- Configuration Management Services
- Capacity Planning and Performance Management Services
- Disaster Recovery Services
- Identity Access Management Services
- Reporting Management Services
- Domain Names Management Services
- Business Analyst Services

Cross Functional Services include lifecycle services that Contractor shall provide across the County Service Frameworks. All requirements, roles and responsibilities described in Cross Functional Services considered to be within the scope for each Service Framework.

2.2. High Level Requirements

2.2.1. Contractor shall provide all Cross Functional Services Framework Components across each Service Framework.

2.2.2. Contractor shall recommend, for County approval, qualified Cross Functional Service Manager as Contractor Key Personnel to ensure delivery and quality of Cross Functional Services.

2.2.3. Contractor shall implement industry leading practices, process, quality, and project methodologies to align processes to people and technology to provide the Services.

2.2.4. Contractor shall develop and submit during Transition, management plans for each Cross Functional Services Framework Component to be included in the Standards and Procedures Manual.

2.2.5. Contractor shall continuously update and submit Cross Functional Services Framework Component management plans, for County approval, and include in the Standards and Procedures Manual.

2.2.6. Contractor shall continuously improve Cross Functional Services by monitoring trends and service quality improvement through independent research and recommending changes annually that improve efficiencies and reduce overall costs.

2.2.7. Contractor shall provide the County with insight into future direction, initiatives, and technology road maps of Third-Parties performing Cross Functional Services.

2.2.8. Contractor shall provide County with Applications, Software and business experience and expertise to support continuous improvement to Cross Functional Services.

2.2.9. Contractor shall provide inventory management across all Cross Functional Services Framework Components to ensure accurate counts, information, consolidated views, etc.

2.3. Contract and Acquisition Management Services

2.3.1. Overview

This section pertains to the Contract and Acquisition Management Services of the Cross Functional Framework. Contract and Acquisition Management Services are the roles and responsibilities for the management of the Agreement, Contractor's relationship with the County and to provide acquisition services.

Contractor's primary responsibilities under Contract and Acquisition Management Services are to:

- Serve as the single point of contact to work with the County to manage the Agreement and all related contracts to provide Operational Services, including disputes, amendments, communications and training.
- Execute and manage the Optional Items Catalog, licenses/support maintenance renewals, subscription renewals, perpetual license renewals, Cloud ASP renewals, Hardware maintenance, Software as a Service (SaaS) renewal, competitively procured Applications Development projects among Contractor sub-contractors and partners.
- Execute Third-Party procurements and market scan / procurement activities.

2.3.2. High Level Requirements

2.3.2.1. Contractor shall provide continuous improvement of Contract and Acquisition Management Services.

2.3.2.2. Contractor shall assign a full-time Contract Manager to act as the single point of contact for the County on all contractual matters, including subcontract(s). The Contract Manager shall cooperatively, promptly and continuously communicate with County-designated staff.

2.3.2.3. Contractor shall deliver quality, high and prompt response Contract Management Services to the County.

2.3.2.4. Contractor shall be responsive and work cooperatively with the County to address requests and resolve issues and disputes.

2.3.2.5. Contractor shall continuously assess the Agreement and recommend improvements to enable the continuous improvement delivery of the Services, with focus on optimizing County's operational performance.

2.3.2.6. Contractor shall work cooperatively to efficiently implement changes to the Agreement.

2.3.2.7. Contractor shall perform procurement activities to support and provide Services and respond to Service Requests (e.g., DAD, OIC, contracts, licenses, etc.).

2.3.2.8. Contractor shall negotiate and enter into contracts with the Third-Parties (except for situations where the Contractor and County agree in advance that the Contract shall be between the County and the Third-Party) upon County approval.

2.3.2.9. Contractor shall create, maintain and post on the Service Portal an accurate inventory of current contracts, procured services, County owner, purchases and other relevant key information that is readily accessible for validation, certifications, reviews and tracking.

2.3.2.10. Contractor shall manage the service catalog (e.g., Third-Party service contracts).

2.3.2.11. Contractor shall maintain a log of all and any purchases with information to track the requesting information to the End-User.

2.3.2.12. Contractor shall provide early notifications to the County point of contact(s) or County department for renewals.

2.3.2.13. Contractor shall manage license, subscriptions, maintenance, certifications agreements to ensure contract and County policy compliance.

2.3.2.14. Contractor shall provide County with requested support for County operational and financial planning information.

2.3.2.15. Contractor shall develop and document in the Standards and Procedures Manual a competitive procurement process that aligns with County competition procedures as outlined below:

- Board of Supervisors Policies A-87 – Competitive Procurement
- Policy A-97 – Protest Procedures for Award of Contracts
- B-39a – Veteran Owned Business (VOB) and Disabled Veterans Business Enterprise (DVBE) Program
- B-53 – Small Business Policy (SBP)

2.3.2.16. Contractor shall solicit market scans and proposals to respond to County-established business requirements and evaluation criteria, and participate with the County in the evaluation against the County-established business requirements and evaluation criteria (including associated integration requirements, if necessary) and shall enter into a contract with the selected Third-Party at the County's direction.

2.3.2.17. Contractor shall provide the County with assessments and recommendations for procurements of services in the cloud, including:

- Develop entry and exit criteria for any engagement with a Third-Party prior to contract signing that identify risks, portability, integration points and relevant impacts
- Develop and provide as part of any solution or procurement one-time and recurring costs, the associated contract terms, Service Levels, liability, insurance and related contract and legal information.
- Ensure the Third-Party meets County policies, regulatory requirements and mandatory requirements

2.3.2.18. Contractor shall create a section in the Standards and Procedures Manual for Contract and Acquisition Management activities and procedures including the procedures that link Contract and

Acquisition Management Services with, Service Desk Services, Applications M&O Services, and Applications Development.

2.3.2.19. Contractor shall annually update and deliver the Contract and Acquisition Management Services Management plan, for County approval, and post on the Service Portal.

2.3.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Contract and Acquisition Management Services.

Contract and Acquisition Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Contract and Acquisition Management policies and procedures.	X	
2. Review and approve Contract and Acquisition Management policies and procedures.		X
3. Produce and submit an overall performance measurement plan to complement the Service Levels. The performance measurement plan shall collect key metrics to enable the County and the Contractor to identify productivity gains, better manage the Services, and provide information for continuous improvement.	X	
4. Review and approve performance measurement plan.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Implement Contract and Acquisition Management policies and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
6. Support Contract and Acquisition Management policies and procedures with necessary staff and resources.	X	
7. Produce and submit a weekly and monthly program status report.	X	
8. Conduct monthly program status reviews with the County including status on the Contractor's achievement of the contractual objectives, specific issues with recommended solutions, and planned activities, and to receive feedback.	X	

Contract and Acquisition Management Roles and Responsibilities		
9. Produce and submit descriptions of contract issues and/or recommended contract PRR on as-needed basis.	X	
10. Review and approve contract PRR.		X
11. Provide program performance metrics to designated County staff members via Service Portal.	X	
12. Provide the County with weekly status updates to apprise relevant parties on the status of backlogged Service Requests and expected resolution dates.	X	
13. Manage relationship contact points with Third-Parties to deliver a single point of contact for the processing and resolution of issues and problems.	X	
14. Assist the County in developing and executing routine reports that allow insight into costs associated with the Agreement.	X	
15. Assist the County in the development of its annual budget by providing: • Current, detailed, and accurate information relating to past operations • Assistance in costing and balancing the implementation of major initiatives • Assistance in spreading the costs of these major initiatives over multiple budget cycles as appropriate • Technical support to determine the impact of changes in technology on costs. • Analysis of usage (i.e., volumes of Resource Unit consumption) and performance • Identification of technical solutions for the reduction of operational costs	X	
16. Produce and submit updates to the County Standards and Procedures Manual.	X	
17. Review and approve updates to the County Standards and Procedures Manual.		X
18. Conduct annual review of existing Third-Party agreements (including cloud applications) to ensure that the County is receiving optimal value from such agreements.	X	

Contract and Acquisition Management Roles and Responsibilities		
19. Review and approve the annual review of existing Third-Party agreements to ensure that the County is receiving optimal value from such agreements.		X

2.4. Integrated Asset Management Services

2.4.1. Overview

This section pertains to the Integrated Asset Management Services Framework Component of the Cross Functional Framework. The Integrated Asset Management Services are the activities and processes associated with tracking, managing, optimizing and continuously improving the overall control and inventory of Assets. Integrated Asset Management Services provides the capabilities to centrally manage all Asset repositories and report across all Assets. Integrated Asset Management Services enable an accounting of all Asset costs, to support strategy, architecture, funding and sourcing decisions.

2.4.2. High Level Requirements

2.4.2.1. Contractor shall acquire and provision all Assets required to perform the Services.

2.4.2.2. Contractor shall provide a County approved Integrated Asset Management System.

2.4.2.3. Contractor shall provide an Integrated Asset Management System that provides centralized management of all integrated Asset repositories including, but not limited to, inventory, financial and contractual data.

2.4.2.4. Contractor shall list ownership of all Assets (e.g., Contractor, County, and Third-Party) in the Integrated Asset Management System.

2.4.2.5. Contractor shall design and deliver an auto-discovery function for all Assets.

2.4.2.6. Contractor shall provide accessibility and search-ability by County for all Integrated Asset Management data.

2.4.2.7. Contractor shall provide monthly reports on all Assets.

2.4.2.8. Contractor shall effectively manage Assets from requisition to retirement.

2.4.2.9. Contractor shall continuously analyze, optimize and leverage County Asset licensing to ensure that the County is in compliance with all license requirements and also that the County is using the most economical number and distribution of licenses.

2.4.2.10. Contractor shall continuously analyze and optimize County maintenance and support agreements to ensure that the County has adequate maintenance and support.

2.4.2.11. Contractor shall identify any unnecessary maintenance and support agreements and promptly terminated.

2.4.2.12. Contractor shall ensure inventory of all Assets are maintained and accurate.

2.4.2.13. Contractor shall provide Integrated Asset Management System reports including Hardware, Software (Desktop Applications Directory and Applications Portfolio) License Compliance, Application and Infrastructure Servers and Personal Computing Assets.

2.4.2.14. Contractor shall optimize pricing and terms for all Third-Party Assets.

2.4.2.15. Contractor shall provide Integrated Asset Management data for analytics for trending, forecasting, planning to facilitate decisions based on Asset information.

2.4.2.16. Contractor shall annually update and deliver the Integrated Asset Management Service Management plan, for County approval, and posted on the Service Portal.

2.4.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Integrated Asset Management Services.

Integrated Asset Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Design and implement an Integrated Asset Management System.	X	
2. Review and approve an Integrated Asset Management System.		X
3. Produce and submit recommended policies, processes and procedures to be added to the Standards and Procedures Manual.	X	
4. Review and approve changes to be added to the Standards and Procedures Manual.		X
5. Produce and submit recommended Asset Management monthly report format (e.g., End-User name, department, account code, location, low-org).	X	
6. Review and approve Asset management monthly report format.		X
7. Produce and submit recommended software license monthly report format.	X	
8. Review and approve recommended software license monthly report format.		X
9. Produce and submit Asset Management policies and procedures.	X	
10. Review and approve Asset Management policies and procedures.		X
11. Produce and submit software license management policies and procedures.	X	
12. Review and approve software license management policies and procedures.		X
13. Produce and submit comprehensive inventory of Assets tracked, managed and reportable through the Asset Management System.	X	
14. Review and Approve comprehensive inventory list provided by the Contractor.		X

Integrated Asset Management Roles and Responsibilities		
Build Roles and Responsibilities	**Contractor**	**County**
15. Develop operational policies standards and procedures manual for security management.	X	
16. Implement Asset Management policies and procedures.	X	
17. Implement Software License management policies and procedures.	X	
18. Implement software License monthly report.	X	
19. Implement Asset Management monthly report.	X	
20. Deploy an electronic Integrated Asset Management System that meets the County's requirements, adheres to defined policies and includes the following asset information (if applicable): • Manufacturer • Model • Serial number • Asset identification number • Asset location • Ownership information (Contractor/County - lease/purchase) • Asset cost information • Maintenance information and history including the age of the Asset and duration of contract terms • Warranty information • Other billing information (e.g., lease information, County-specific information) • Transaction edit history (e.g., locations, billing and User)	X	
21. Provide and support an electronic Integrated Asset Management System which includes asset auto discovery tools to maintain asset data and User profiles.	X	
22. Provide acquisition and tracking as required to fulfill County requests.	X	
23. Negotiate, enter into, track and manage all contracts, including licenses, with Third-Parties as required for the provision of the Services.	X	
24. Provide and support an electronic interface to the County's finance and chargeback systems to meet accounting, tracking, and reporting requirements.	X	
25. Develop and implement online access to Asset Management information.	X	

Integrated Asset Management Roles and Responsibilities		
26. Implement and support interfaces to feed asset location and financial data, including Third-Party data such as relevant taxation, book and depreciation value data to an online reporting dashboard.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Track and manage all Assets provided by the Contractor.	X	
28. Conduct periodic reviews and provide exception reports resulting from use of asset auto discovery tools.	X	
29. Produce and submit monthly reports on Assets.	X	
30. Produce and submit copies of all Third-Party contracts, including licenses, upon request of the County.	X	
31. Produce and submit monthly software license management report.	X	
32. Review and approve monthly software license management report.		X
33. Validate compliance with applicable software licensing agreements using automated software tools and manual processes as required.	X	
34. Verify installed software for non-networked PCs (that periodically touch the network to check E-Mail, for example), while those PCs are in contact with the network.	X	
35. Report any license compliance issues no more than 30 days from the date of the issue.	X	
36. Report on contract expirations, license changes/upgrades, etc. in advance to prevent disruptions in service, non-compliance issues, etc.	X	
37. Report any expiration or renewal requirements for Assets to allow for planning and mitigation.	X	
38. Manage the ordering, procurement and delivery processes in compliance with County procurement and acceptance processes.	X	
39. Maintain version control on asset inventory.	X	
40. Dispose Assets (e.g. donation, sale, disposal) per County direction and generally acceptable accounting and financial standards or requirements.	X	
41. Provide reports of Asset Management review results.	X	

Integrated Asset Management Roles and Responsibilities		
42. Provide and, upon County approval, implement Asset Management remediation plan for Asset Management deficiencies.	X	
43. Review and approve review reports and remediation plans of Asset inventory management information.		X
44. Provide reports of County asset financial information including depreciation, maintenance contracts and value of Assets.	X	
45. Conduct periodic/ad hoc quality assurance review of Integrated Asset Management System.		X

2.5. Billing Management Services

2.5.1. Overview

Billing Management Services consist of the activities and processes associated with the timely and accurate billing for the Services. Billing Management Services shall collect consumption data for all Frameworks, calculate all charges and billing information, produce and provide invoices to the County, provide chargeback details that meet the County's requirements, and provide all necessary support to ensure the timely and accurate processing of both the invoice and chargeback.

2.5.2. High Level Requirements

2.5.2.1. Contractor shall digitally interface its Contractor billing system with the County chargeback management system (iTrack).

2.5.2.2. Contractor shall manage and support the operational availability of the iTrack to Oracle Financials interface.

2.5.2.3. Contractor shall use a billing program that efficiently and effectively handles the tracking of billable resources and maintains a direct interface to the Integrated Asset Management Services.

2.5.2.4. Contractor shall make provide, for County approval, all process and procedural documentation pertaining to Billing Management Services.

2.5.2.5. Contractor shall provide accurate and timely invoices with an appropriate level of detail.

2.5.2.6. Contractor shall promptly provide accurate and timely detailed electronic billing information that facilitates the County's chargeback activities.

2.5.2.7. Contractor shall support all activities required to review, validate, substantiate, and detail its billings.

2.5.2.8. Contractor shall work with the County to optimize the invoice and chargeback process, including continuous improvement of reporting and automation.

2.5.2.9. Contractor shall communicate to County information impacting the billing of resources.

2.5.2.10. Contractor shall provide details for any billing inquiries to support the costs billed to the County or invoiced to the County upon request.

2.5.2.11. Contractor shall annually update and deliver the Billing Management Services Management plan, for County approval, and posted on the Service Portal.

2.5.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Billing Management Services.

Billing Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommended policies, processes and procedures to be added to the Standards and Procedures Manual.	X	
2. Review and approve changes to be added to the Standards and Procedures Manual.		X
3. Identify chargeback and reporting requirements.		X

Billing Management Services Roles and Responsibilities		
4. Identify monthly invoicing requirements.		X
5. Produce and submit recommended monthly invoice/billing report format in accordance with County requirements.	X	
6. Review and approve monthly billing report format.		X
7. Document and maintain invoicing requirements.	X	
8. Participate in, and support, billing reviews as requested by the County.	X	
Build Roles and Responsibilities	**Contractor**	**County**
9. Provide an automated interface with the County's finance system for Billing Management Services.	X	
10. Provide an automated interface with the County's chargeback system in accordance with County requirements, including the ability for the County to review the chargeback reports and supporting data online through the Service Portal without any delays.	X	
11. Produce and submit monthly reports (both hardcopy and electronically) detailing all usage and charges.	X	
12. Maintain an electronic repository of all Billing Management records (reports, invoices, chargeback, etc.) for the duration of the contract.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
13. Contractor shall verify staff enter billable time on a daily basis for accurate tracking of project costs.	X	
14. Produce and submit to County chargeback reports and monthly invoices.	X	
15. On a monthly basis, meet with the County's finance staff to review invoices including: • Provide a mock invoice for review and agreement • If discrepancies are identified, clarify and resolve them • Meet again within a week to reach agreement on the changes or clarifications so the submitted invoice can be signed off	X	
16. Approve chargeback reports.		X
17. Download on a monthly basis all usage and charge information to the County chargeback application.	X	
18. Provide invoices per County requirements.	X	

Billing Management Services Roles and Responsibilities		
19. Document and maintain County chargeback reporting requirements.	X	
20. Calculate, report, and chargeback all applicable taxes and provide monthly billing for current and past services as well as track payments and balances.	X	
21. Provide the billing data needed to reconcile bills.	X	
22. Approve invoices.		X
23. Maintain and provide an electronic archive of all billing and its details.	X	
24. Retain all source system data used for billing to provide audits trails or verification of details for the duration of the Agreement.	X	

2.6. Security Management Services

2.6.1. Overview

The Security Management Services Framework Component within the Cross Functional Framework applies to the discipline of designing, implementing and maturing security practices to protect critical County business processes and Assets across the enterprise.

2.6.2. High Level Requirements

2.6.2.1. Contractor shall provide the continuous improvement in overall security services that protect the County.

2.6.2.2. Contractor shall provide a qualified Chief Information Security Officer (CISO), with County approved, that will work directly with the County CISO.

2.6.2.3. Contractor shall ensure Contractor assigned CISO is not directly involved in the management of day-to-day operations.

2.6.2.4. Contractor CISO shall work with the Contractor assigned CTA to ensure strategic alignment with architecture standards and guidelines.

2.6.2.5. Contractor shall develop strategic risk guidance for Service Requests, including the evaluation and recommendation for technical controls.

2.6.2.6. Contractor shall participate in architecture and strategy sessions with the County to determine and maintain the Security Management roadmap.

2.6.2.7. Contractor shall work with each Service Framework to ensure alignment, training, validation, compliance with Security Management Services.

2.6.2.8. Contractor shall ensure confidentiality of all Hardware and Software used to provide the Services.

2.6.2.9. Contractor shall ensure the availability of all Hardware and Software providing the Services is only used for its intended purpose.

2.6.2.10. Contractor shall design, develop, procure, implement and monitor a strategic, and continuously improving comprehensive security and risk management program to protect the integrity, confidentiality and availability of County Data and the Services.

2.6.2.11. Contractor shall establish a hierarchical security governance program that includes the formation of an information security steering committee which includes the County and Contractor staff and provides for the centralized governance of security services.

2.6.2.12. Contractor shall design, develop, implement, maintain and publish up-to-date information security policies, procedures, training, standards and guidelines to the Service Portal.

2.6.2.13. Contractor shall, with County CISO approval, create and manage information security and risk management awareness training programs for End-Users, Third-Party and approved system users.

2.6.2.14. Contractor shall design, develop, implement and maintain risk assessment and risk management processes for the Services.

2.6.2.15. Contractor shall, with the County CISO approval, design, develop and maintain categories for information ownership, classification, accountability and protection.

2.6.2.16. Contractor shall continuously assess and improve the Security Management Services against an industry-standard maturity model.

2.6.2.17. Contractor shall perform all necessary security-related reviews and annually attest to security compliance for delivering the Services.

2.6.2.18. Contractor shall use the NIST Computer Security Resource Center (CSRC) security framework as a guide for Security Management Services.

2.6.2.19. Contractor shall continuously monitor security and risk environmental factors for evolving trends and threats.

2.6.2.20. Contractor shall develop and implement plans to remediate any identified threat.

2.6.2.21. Contractor shall develop and maintain an annual Security life cycle report for the Services.

2.6.2.22. Contractor shall design, develop, implement and maintain a security incident management and response plan, for County approval, and post to the Service Portal.

2.6.2.23. Contractor shall provide periodic executive reports on the "State of Security" which includes the overall effectiveness, efficiency, maturity and other relevant matters related to the Services.

2.6.2.24. Contractor shall develop a security information and event management (SIEM) solution and the required set of operational procedures in defining, using and maturing the processes.

2.6.2.25. Contractor shall maintain Federal and State compliance to security for any applicable County program, application or other Service.

2.6.2.26. Contractor shall annually update and deliver the Security Management Services Management plan, for County approval, and posted on the Service Portal.

2.6.2.27. Contractor shall provide the Enterprise Application Access (EAA) solution.

2.6.2.27.1. EAA integrates data path protection, identity and access management (IAM), application security, multi-factor authentication (MFA), single sign-on (SSO), and management visibility and control into a unified service across all application locations and types (on-premises, Internet, IaaS, SaaS, etc.).

2.6.2.27.2. EAA will be implemented on all active applications (PA, CA, IA) to the enterprise portal.

2.6.2.27.3. EAA will be implemented on all County departments, San Diego County Sheriff Department, San Diego County District Attorney and San Diego County Employees Retirement Association and be available to associated subcontractors, partners and citizens in support of the County.

2.6.2.28. Contractor shall provide the Multi-Factor Authentication (MFA) solution.

2.6.2.28.1. The MFA Service integrates with County EAA solution to provide advanced multi-function authentication functionality across all County applications using supported EAA MFA methods (e.g., FIDO/FIDO2; SMS; Hardware OTP; Software OTP; Push).

2.6.2.28.2. The MFA Service is implemented across all County departments for users of County shared applications including County subcontractors performing work on

behalf of County, partners and Contractor staff supporting the Agreement.

2.6.2.28.3. The County EAA Service is extended to the County of San Diego Sheriff's Department, County of San Diego District Attorney's Office and to San Diego County Employees Retirement Association, to the extent required to access County applications using the County MFA solution.

2.6.2.29. Contractor shall provide the Malware Protection solution to all County websites protected by the Akamai Web Application Firewalls.

2.6.2.29.1. Malware Protection shall protect web apps and Application Programming Interface (APIs) from malicious file uploads by scanning file uploads at the Akamai edge.

2.6.2.29.2. Malware Protection shall integrate with Akamai Web Application Firewall to detect and block malware at the Akamai edge by scanning files once, at the edge, to avoid setting scanning at every application.

2.6.2.30. Contractor shall provide the Secure Internet Access (SIA) solution to all County managed devices.

2.6.2.30.1. SIA shall provide a cloud-based secure web gateway (SWG) that protects County network.

2.6.2.30.2. SIA shall proactively block requests to known malware, phishing, command and control, and Domain Name System (DNS) data exfiltration domains.

2.6.2.30.3. SIA shall block malicious payload downloads with improved zero-day protection before they compromise endpoint devices.

2.6.2.30.4. SIA shall protect devices when on and off the network, including mobile devices.

2.6.2.30.5. SIA shall protect all outbound DNS traffic including Internet of Things (IoT), servers and peripherals.

2.6.2.30.6. SIA shall provide detection/prevention of zero-day phishing attacks.

2.6.2.30.7. SIA shall enforce acceptable use policies.

2.6.2.30.8. SIA shall block categories of domains.

2.6.2.30.9. SIA shall provide visibility and control over internet-based applications, such as social media.

2.6.2.30.10. SIA shall control the types of files that can be uploaded/downloaded on the internet.

2.6.2.30.11. SIA shall provide web-based Data Loss Prevention (DLP) controls.

2.6.2.30.12. SIA shall include tools to identify the specific devices on the network making requests that violate the configured policy.

2.6.3. Environment

The environment scope of Security Management Services includes, but is not limited to, the following:

2.6.3.1. Technical

2.6.3.1.1. Approve appropriate methods for the protection of all Assets used for the Services.

2.6.3.1.2. Propose authentication methods, password policy, encryption methods, etc.

2.6.3.1.3. Propose rules for secure teleworking.

2.6.3.1.4. Define required security features of Internet services.

2.6.3.1.5. Define principles for secure development of information systems.

2.6.3.1.6. Review logs of user activities in order to recognize suspicious behavior.

2.6.3.2. Business continuity

2.6.3.2.1. Coordinate the business impact analysis process and the creation of response plans.

2.6.3.2.2. Coordinate exercising and testing.

2.6.3.2.3. Perform post-Incident review of the recovery plans.

2.6.3.3. Compliance

2.6.3.3.1. Develop the list of interested parties related to information security.

2.6.3.3.2. Develop the list of requirements from interested parties.

2.6.3.3.3. Remain in continuous contact with authorities.

2.6.3.3.4. Coordinate all efforts related to personal data protection.

2.6.3.4. Risk management

2.6.3.4.1. Develop Contractor training on performing risk assessment.

2.6.3.4.2. Coordinate the process of risk assessment.

2.6.3.4.3. Propose the selection of safeguards.

2.6.3.4.4. Propose the deadlines for safeguards implementation.

2.6.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Security Management Services.

Security Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define County requirements at the enterprise level for all security services (e.g., business, technology strategy, functional, availability, capacity, performance, applications, backup and continuity service).		X
2. Assist in developing Security standards, policies and procedures including leading industry practices.	X	
3. Produce and submit quarterly updates to security requirements, standards, procedures and policies including regulatory requirements for County approval.	X	
4. Review and approve security requirements, standards, procedures and policies for County.		X
5. Develop security patching standards relevant to the environment including asset management integration with Third-Party security vulnerability notifications services (e.g., NIST NVD).	X	
6. Review and approve security patching standards relevant to the environment.		X
7. Perform feasibility studies for the implementation of new security technologies that best meet County business needs and meet cost, performance and quality objectives.	X	

Security Management Roles and Responsibilities		
8. Participate in technical and business planning sessions to establish security standards, architecture and project initiatives.	X	
9. Conduct technical reviews and provide recommendations for improvements to the infrastructure, application development and operations that increase the overall effectiveness, efficiency and prudent resource and cost management of security.	X	
10. Produce and submit operational policies and procedures for Security Management.	X	
11. Review and approve operational policies and procedures for Security Management.		X
12. Recommend appropriate controls for individual departments that meet requirements (e.g., HIPAA, HHSA, etc.).	X	
13. Review and approve appropriate controls for individual departments meet requirements (e.g., HIPAA, HHSA, etc.).		X
14. Recommend Security Management testing and vulnerability analysis standards on a yearly basis.	X	
15. Review and approve Security Management testing and vulnerability analysis standards on a yearly basis.		X
16. Produce and submit policies and procedures for relevant to the Services and are necessary for protecting the Confidentiality, Integrity and Availability of Assets, information and resources.	X	
17. Review and approve policies and procedures for relevant to the Services and are necessary for protecting the Confidentiality, Integrity and Availability of Assets, information and resources.		X
18. Produce and submit annual security strategies and roadmaps for the Services.	X	
19. Review and approve annual security strategies and roadmaps for the Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
20. Develop and maintain a Security and Risk Management Manual.	X	
21. Review and approve the Security and Risk Management Manual.		X
22. Develop and maintain a Risk Assessment Process and Procedure Manual.	X	

Security Management Roles and Responsibilities		
23. Review and approve the Risk Assessment Process and Procedure Manual.		X
24. Identify relevant and applicable standards and methods to apply to County systems and applications to meet all special statutory and regulatory objectives and requirements.	X	
25. Comply with all statutory and regulatory requirements associated with the delivery of the Services, requirements regarding systems, including specific regulatory requirements for systems affiliated with the California Law Enforcement Telecommunications System (CLETS) and the FBI Criminal Justice Information Systems (CJIS).	X	
26. Evaluate and provide risk reduction and cost effectiveness of security processes and procedures.		X
27. Review all security patches relevant to the environment and classify the need and speed in which the security patches must be installed.	X	
28. Maintain all documentation required for security reviews and internal control and control testing.	X	
29. Recommend encryption technologies, security monitoring, anti-virus programs and relevant patches and upgrades as required by County policies and standards.	X	
30. Review and approve encryption technologies, security monitoring, anti-virus programs and relevant patches and upgrades as required by County policies and standards.		X
31. Design a web-based security dashboard that displays metrics, aggregated security log data across all frameworks, and enable total security awareness of the County's security environment.	X	
32. Review and approve the web-based security dashboard that displays metrics, aggregated security log data, and enable total security awareness of the County's security environment.		X
33. Develop and recommend improvement plans for Locations as needed to maintain effective physical security.	X	
34. Review and approve physical security improvement plans for Locations.		X
35. Develop and document technical design plans and environment configuration based on County security requirements.	X	

Security Management Roles and Responsibilities		
36. Review and approve all adjustments to County security policies, regulations and procedures as a result of new service features and components.		X
37. Produce and submit System and Application security procedures.	X	
38. Review and approve System and Application security procedures.		X
Operate Roles and Responsibilities	**Contractor**	**County**
39. Conduct security assessments and report monthly on vulnerabilities and recommended mitigations.	X	
40. Conduct scheduled review meetings between the Contractor's security officer and the County security officer and related security working group(s).	X	
41. Support County requested internal and Third-Party security reviews, vulnerability and penetration testing.	X	
42. Support periodic reviews of security practices, process and procedures as required by County.	X	
43. Review the County's security policies annually and work with the County security officer to recommend updates, additions, or changes as the County's working environment changes.	X	
44. Develop and maintain a Security Risk Registry of all identified County security risks.	X	
45. Create and maintain a secured online repository for all Security related documents and artifacts (e.g., Customer Service Request Forms, Security Assessments, Security Audits, Security Roadmaps, Risk Assessments, etc.).	X	
46. Review and validate management and current updates are performed to the Security on-line repository.		X

2.7. Service Delivery Management (SDM) Services

2.7.1. Overview

This section pertains to Service Delivery Management Services Cross Functional Framework Component. Each County Business Group (FG3, CSG, PSG, HHSA and LUEG) has a single, assigned Service Delivery Manager. The Service Delivery Manager(s) shall act as a liaison to the Business Group with respect to all Services, including but not

limited to, operational support, billing management, escalation management, change management, release management, Incident management, Problem management, availability and capacity management, Service Request status, communications and service continuity in the event of unplanned outages, declared emergency or disaster.

The Enterprise Service Delivery Manager shall interface directly to the CTO and shall coordinate the delivery of Services to the assigned Business Group Service Delivery Managers. The Business Group Service Delivery Manager shall continuously receive and assess customer feedback in order to improve overall service delivery goals.

2.7.2. High Level Requirements

2.7.2.1. Contractor shall recommend, for County approval, a qualified Service Delivery Manager as Contractor Key Personnel that reports to CTO.

2.7.2.2. Contractor shall recommend, for County approval, qualified Business Group Service Delivery Managers as Contractor Key Personnel to manage Service Delivery Management Services.

2.7.2.3. Contractor Service Delivery Manager shall be familiar with ITIL and have experiences in a variety of frameworks including but not limited to, Service Desk, End-User Services, Network Management, Data Center Management, Change Management, Program Management, application delivery, and Release Management.

2.7.2.4. Contractor shall define and maintain, for County approval, processes for all Service Delivery Manager Services.

2.7.2.5. Contractor Service Delivery Managers shall maintain and build relationships with County Business Groups and departments.

2.7.2.6. Contractor Service Delivery Managers shall handle all Incident and Problem escalations and trending to provide consistency to the level of service quality.

2.7.2.7. Contractor shall work collaboratively with the County to ensure the most efficient and effective use of SDM resources and processes.

2.7.2.8. Contractor shall annually update and deliver the Service Delivery Management Service Management plan, for County approval, and posted on the Service Portal.

2.7.3. Contract and Acquisition Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with SDM Services.

SDM Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop SDM job standards and requirements.	X	
2. Review and approve SDM job standards and requirements.		X
3. Provide resumes of SDMs meeting the approved standards and requirements.	X	
4. Select a SDMs meeting the approved standards and requirements.		X
5. Produce and submit SDM Services policies and procedures.	X	
6. Review and approve SDM Services policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Implement SDM Services policies and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
8. Perform internal SDM activities to ensure a high-level of performance and quality across all Service Frameworks.	X	
9. Audit Contractor Operations and Maintenance activities for compliance with Operational policies & procedures.		X
10. Produce and submit results of internal reviews relating to the County's service frameworks.	X	
11. Review and approve internal review findings.		X
12. Incorporate review findings into County Service frameworks as necessary to maintain compliance.	X	

SDM Management Roles and Responsibilities		
13. Recommend resolutions to address recurring operational Problems or Incidents.	X	
14. Review and approve resolutions to address recurring operational Problems or Incidents.		X
15. Track and report recurring operational Problems or Incidents and provide associated consequences of Problems or Incidents if there is a business impact to the County.	X	
16. Ensure that recurring operational Incidents are reviewed using root cause analysis processes and implement corrective actions as appropriate.	X	
17. Routinely assess customer satisfaction at program and service element levels using automated survey tool.	X	
18. Initiate additional survey processes as required to measure Contractor's performance rating.		X
19. Report results and trend analysis of customer satisfaction surveys with corrective action plans, as needed, in the monthly status report.	X	
20. Periodically review selected functions to verify that established policies and procedures are being followed and, if variances are noted, recommend corrective actions.	X	
21. Perform periodic internal reviews to check that standards are being followed.	X	
22. Perform regular reviews of Contractors services and performance against Service Levels and other performance measures.	X	
23. Lead and manage internal delivery teams to review incidents, problems and any other operational Incidents affecting client production and non-production environments.	X	
24. Drive the Contractor teams to remediate the problems and provide root cause analysis as needed.	X	
25. Review change management requests and participate in Change Management Boards.	X	
26. Provide a consolidated monthly report on service delivery information, challenges and insights.	X	

2.8. [Reserved]

2.9. Project Management Services

2.9.1. Overview

Project Management Services defines the structured effort to manage risk that achieves expected results. Project Management Services shall deliver products, Assets, change and/or components within agreed resources and a defined start and end time.

2.9.2. High Level Requirements

2.9.2.1. Contractor shall provide qualified program and project management resources with relevant background and experience including PMI certification.

2.9.2.2. Contractor shall recommend, for County approval, qualified Project Management Office Manager as Contractor Key Personnel to manage Project Management Services.

2.9.2.3. Contractor PMO shall report directly to the Contractor Account Management team.

2.9.2.4. Contractor PMO shall establish continuous mentoring and training for Project Managers.

2.9.2.5. Contractor shall define standards, methods and best practices that shall be used in the delivery of Project Management Services.

2.9.2.6. Contractor shall establish centralized tracking and reporting for all projects accessible from the Service Portal.

2.9.2.7. Contractor shall define all processes in the delivery of Project Management Services and that are posted on the Service Portal.

2.9.2.8. Contractor shall define measurements to ensure the delivery of projects on time, on budget and in scope.

2.9.2.9. Contractor shall implement, with County approval, a standardized project management methodology that incorporates industry typical practices. This methodology shall be used by the Contractor in providing all of the Services.

2.9.2.10. Contractor shall annually update and deliver the Project Management Services Management plan, for County approval, and posted on the Service Portal.

2.9.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Project Management Services.

Project Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for standard project management tools, reports, and artifacts.	X	
2. Review and approve standard project management tools, reports, and artifacts.		X
3. Produce and submit recommendations for project-specific tools and artifacts.	X	
4. Review and approve project-specific tools and artifacts.		X
5. Produce and submit resource-loaded project plans for all projects.	X	
6. Review and approve resource-loaded project plans for all projects.		X
7. Produce and submit project status reports on no less than a monthly basis.	X	
8. Provide a range of training options in the service catalog.	X	
9. Produce and submit project management policies and procedures.	X	
10. Review and approve project management policies and procedures.		X
11. Recommend business process reengineering methodologies.	X	

Project Management Roles and Responsibilities		
12. Assess and approve business process re-engineering methodologies.		X
13. Identify opportunities for business process improvements.	X	
14. Provide industry knowledge applicable to County departmental business to identify opportunities for business process reengineering and Application development and integration/modification.	X	
Build Roles and Responsibilities	**Contractor**	**County**
15. Develop operational policies standards and procedures manual for Project Management Services.	X	
16. Implement County authorized Project Management discipline.	X	
17. Work in conjunction with the County's training and development resources to provide a common look and feel to training delivery methods.	X	
18. Implement and manage County-authorized Project Management tools and processes based on industry standards.	X	
19. Develop and maintain a training course catalog in cooperation with County HR and the Business Groups to provide End-Users access to training so they can develop the necessary skills to fulfill their responsibilities.	X	
20. Implement approved project management policies and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
21. Support project management policies and procedures.	X	
22. Provide high quality project management for all initiatives and projects undertaken as part of the Services.	X	
23. Participate in Program management and Project management activities as required to ensure successful work efforts.		X
24. Facilitate project status reviews with County management and staff on no less than a monthly basis.	X	
25. Track projects through timekeeping tool and biweekly status reports.	X	
26. Distribute the standard project processes, templates, or other vehicles, to all stakeholders to collect relevant project operational and performance data.	X	

Project Management Roles and Responsibilities		
27. Support the County's Verification & Validation activities including assisting in identifying errors, risk factors, omissions, discrepancies, constraints, performance and security Incidents, and other obstacles in project implementations.	X	
28. Provide local venues for training, particularly for Cross-Functional Services training or special purpose training when delivering training to Users in their environment is not practical (e.g., when providing training on new systems or applications for which a computer laboratory type environment is necessary and shall be leveraged across many training sessions).	X	
29. Provide project planning, tracking and management of project activities.	X	
30. Document project lessons learned and summarize the outcomes of the project.	X	
31. Ensure that all changes to the project are reviewed and approved in advance by coordinating all changes across the project and notifying stakeholders of approved changes.	X	
32. Approve project changes.		X
33. Examine project issues to determine their impact to the analysis or project effort.	X	
34. Categorize risks within a project and analyze as to the consequences, probability, impact, exposure, mitigation, contingency and triggers.	X	

2.10. Integration and Testing Services

2.10.1. Overview

Integration and Testing Services are the activities associated with ensuring that all individual components configured with or added to the environment work together cohesively to achieve the intended results. The following table identifies the Integration and Testing roles and responsibilities that Contractor and County shall perform.

2.10.2. High Level Requirements

2.10.2.1. Contractor shall conduct tests integration or interfaces between components, interactions to different parts of the system such as an

operating system, file system and hardware or interfaces between systems.

2.10.2.2. Contractor shall develop and deliver, for County approval, and implement a methodology and tool sets for conducting Integration and Testing Services.

2.10.2.3. Contractor shall update annually the methodology for conducting Integration and Testing Services.

2.10.2.4. Contractor shall continuously update tools sets used for conducting Integration and Testing Services.

2.10.2.5. Contractor shall verify functional, performance, and reliability requirements are placed on major design items.

2.10.2.6. Contractor shall detect any inconsistencies between the software units integrated together or between any of the instances of the standard hardware.

2.10.2.7. Contractor shall define and maintain, for County approval, processes for all Integration and Testing Services

2.10.2.8. Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.10.2.9. Contractor shall annually update and deliver the Integration and Testing Services Management plan, for County approval, and posted on the Service Portal.

2.10.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Integration and Testing.

Integration and Testing Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Integration and Testing Services Roles and Responsibilities		
1. Define Integration and Testing requirements and policies.		X
2. Develop, document and maintain in the Standards and Procedures Manual Integration and Testing procedures that meet requirements and adhere to defined policies.	X	
3. Review and approve Integration and Testing procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Develop operational policies standards and procedures manual for Integration and Testing.	X	
5. Define Test requirements.		X
6. Manage and schedule integration test environment.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Maintain software release matrices across development, QA, and production environments and Networks.	X	
8. Validate and approve the software release matrix.		X
9. Evaluate all new and upgraded components or services for compliance with County security policies, regulations and procedures.	X	
10. Validate new and upgraded components or services for compliance with County security policies, regulations and procedures, as required.		X
11. Assess and communicate the overall impact and potential risk to components prior to testing completion.	X	
12. Conduct integration and security testing for all new and upgraded equipment, Networks, software or services to include unit, system, integration and regression testing based on requirements defined in requirements and design documents.	X	
13. Stage new and upgraded equipment, software or services to smoothly transition into existing environment based on requirements defined in requirements and design documents.	X	
14. Perform modifications and performance-enhancement adjustments to County system software and utilities as a result of changes to architectural standards or additions and upgrades to the environment.	X	

Integration and Testing Services Roles and Responsibilities		
15. Test new releases of supported Hardware and Software to ensure required performance and functionality is maintained in conformance with County Service Levels.	X	
16. Provide Middleware required to integrate Software and Hardware.	X	
17. Support Middleware required to integrate Software and Hardware.	X	
18. Provide integration of application software.	X	

2.11. Incident Management Services

2.11.1. Overview

Incident Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with restoring service operations to County End-Users. Incident Management will restore unplanned disruption to the Services as quickly as possible while providing minimal impact to County business operations. An Incident is any unplanned event, which causes an interruption or a reduction to the quality of the Services.

The Service Desk is responsible for primary ownership of recording and tracking all Incidents and is responsible for the close coordination and ongoing monitoring and tracking of, and reporting on, Incidents. The Service Desk shall be responsible for escalating Incidents and coordinating with all appropriate Tier 2, Tier 3 and Tier 4 support groups.

The Incident Management processes and activities are inter-related and complementary with Change Management, Release Management and Configuration Management, as well as Problem Management.

2.11.2. High Level Requirements

2.11.2.1. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and processes related to Incident Management Services.

2.11.2.2. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Incident Management methodology.

2.11.2.3. Contractor shall own, record and track all Incidents end-to-end.

2.11.2.4. Contractor shall follow all defined Service Level priorities for all Incidents.

2.11.2.5. Contractor shall assume the highest severity for any Incident lacking complete clarity.

2.11.2.6. Contractor shall immediately communicate with the County CTO of all Severity 1 and Severity 2 Incidents.

2.11.2.7. Contractor shall define, document and continuously maintain an Incident Response Team for all Severity 1 and Severity 2 Incidents.

2.11.2.8. Contractor shall investigation and diagnosis all Incidents.

2.11.2.9. Contractor shall develop and deliver an RCA for all Severity 1 and Severity 2 Incidents or ad-hoc Incidents as requested by County.

2.11.2.10. Contractor shall develop and post escalation procedures for Incidents Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.11.2.11. Contractor shall annually update and deliver the Incident Management Services Management plan, for County approval, and posted on the Service Portal.

2.11.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Incident Management Services.

Incident Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Establish criteria for Incident Management support requirements, including equipment and services to be covered, severity levels, definitions and characteristics, Incident classification and prioritization schema, escalation requirements.		X

Incident Management Services Roles and Responsibilities		
2. Develop Incident Management policies, process and procedures that support County's Incident Management support requirements.	X	
3. Review and approve Incident Management policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Develop operational policies standards and procedures manual for Incident Management.	X	
5. Provide and continuously maintain an Incident Management system and knowledge management database, including all Hardware, Software, databases, automated monitoring tools, and management and reporting tools, which are acceptable to County.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
6. Provide unrestricted read access by County-authorized staff and other personnel to all current and historical Incident records and knowledgebase data.	X	
7. Monitor the Incident Management system for automatically generated and logged Incident alerts and events.	X	
8. Resolve Incidents on the first call in accordance with the Procedures Manual, knowledge database documents, and configuration database(s).	X	
9. Identify, filter, and classify Events and Incidents to a severity level and handle according to agreed-upon Incident response procedures.	X	
10. Diagnose and resolve Incidents; where possible use desktop remote control with user's approval and disconnecting when complete. Where possible, implement appropriate corrective actions for known errors (e.g., workarounds for known unresolved Incidents).	X	
11. Escalate Incidents to the appropriate next-level service group within Contractor, County, or Third-Party service as soon as it is clear that the Incident is unable to be resolved without additional assistance or as required to comply with Service Level response times.	X	
12. Monitor and track Incident resolution progress through to final closure and record/update Incident record status as appropriate.	X	

Incident Management Services Roles and Responsibilities		
13. Provide expert functional and process assistance for applications at Tier 1 and escalate to Tier 2 or 3 resource as required.	X	
14. Provide Tier 1 assistance to inquiries on the features, functions and usage of Hardware and Software.	X	
15. Provide Tier 1 support for applications software on the supported applications.	X	
16. Propose training and Tier 1 scripts and workarounds for the Service Desk for applications software on the approved list.	X	
17. Approve training and Tier 1 scripts and workarounds for the Service Desk for applications software on the approved list.		X
18. Provide Tier 2 and Tier 3 support for Applications software on the supported applications list.	X	
19. Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed/resolved Incident.	X	
20. Assist End-Users with questions relating to functionality and use of End-User Hardware and Software.	X	
21. Document solutions to resolved Incidents in central knowledgebase. Accurately update all information pertinent to Incidents including general verbiage, codes, et al.	X	
22. Notify designated County personnel of all Severity 1 and Severity 2 Incidents within the designated timeframe.	X	
23. Contact designated County business personnel of applicable Severity 1 and Severity 2 Incidents.		X
24. Maintain current and historical records of all calls and the resolution of those calls for the life of the contract and provide reporting and trends.	X	
25. Troubleshoot, diagnose and resolve Incidents for all Hardware and Software warranty and non-warranty devices, including removing and / or repairing physically broken or inoperable devices.	X	
26. Provide Dispatch for End-User devices as required.	X	
27. Provide end-to-end Incident Identification, Escalation and Resolution Management; and a Closure Process including the management of those Incidents escalated to Third-Parties.	X	

Incident Management Services Roles and Responsibilities		
28. Track ongoing status of any Incident and their corresponding Incident record to ensure that identified Incidents are addressed and resolved.	X	
29. Ensure Incident resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.	X	
30. Coordinate and take ownership of Incident resolution across all Frameworks with County and Third-Parties.	X	
31. Periodically review the status of open, unresolved Incidents and related Incidents and the progress being made in addressing Incidents.	X	
32. Participate in Incident Management review sessions as appropriate.	X	
33. Conduct Incident review sessions and provide listing and status of same categorized by Incident severity impact.	X	
34. Participate in Incident Management review sessions.		X
35. Coordinate with County and Third-Party Tier 2 support groups to acquire and transfer knowledge on Incident resolution and record this knowledge gained into the knowledge base to facilitate increased ability for Third-Party Tier 1 Service Desk in providing first-call resolution.	X	
36. Conduct follow-up with End-Users who reported the Incident to verify that the Incident was resolved to the End-User satisfaction.	X	
37. Close out Incidents that were resolved satisfactorily.	X	
38. Provide Incident Management reporting as required.	X	

2.12. Problem Management Services

2.12.1. Overview

Problem Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated of resolving not-yet-known root cause behind one or more Incidents.

The Problem Management processes and activities are inter-related and complementary with Change Management, Release Management and Configuration Management, as well as Incident Management.

2.12.2. High Level Requirements

2.12.2.1. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and processes related to Problem Management Services.

2.12.2.2. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Problem Management Services methodology.

2.12.2.3. Contractor shall own all reported or diagnosed Problems end-to-end.

2.12.2.4. Contractor shall develop and implement proactive problem management for Incidents and identify trends to prevent future Incidents.

2.12.2.5. Contractor shall provide Problem Management Services for all identified Problems and systemic Incidents related to the Services.

2.12.2.6. Contractor shall provide coordination and assistance to Third-Party in performing for Problem Management Services.

2.12.2.7. Contractor shall provide reactive Problem Management Services by diagnosing and solving Problems in response to one or more Incidents.

2.12.2.8. Contractor shall maintain, update and report information about Problems and the appropriate workarounds and resolutions.

2.12.2.9. Contractor shall continuously work to reduce the number and impact of Incidents and Problems occurring within the County.

2.12.2.10. Contractor shall be responsible for ensuring that resolutions to Problems are implemented in a timely fashion.

2.12.2.11. Contractor shall fully document and deliver, for County review, all Problems including symptoms through final resolution.

2.12.2.12. Contractor shall prevent recurrence of Incidents related to these errors by determining the unknown underlying cause (e.g., root cause) and resolving them.

2.12.2.13. Contractor shall annually update and deliver the Problem Management Services Management plan, for County approval, and posted on the Service Portal.

2.12.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Problem Management Services.

Problem Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define requirements and policies for Problem Management (e.g., events that trigger a Root Cause Analysis (RCA), categorization and prioritization schema, etc.).		X
2. Participate in developing Problem Management requirements and policies.	X	
3. Develop appropriate process and procedures and methodologies that support County-approved Problem Management requirements and policies that comply with County requirements.	X	
4. Approve appropriate process and procedures and methodologies that support County-approved Problem Management requirements and policies that comply with County requirements.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Develop operational policies standards and procedures manual for Problem Management.	X	

Problem Management Services Roles and Responsibilities		
6. Implement appropriate process and procedures and methodologies that support County-approved Problem Management requirements and policies that comply with County requirements.	X	
7. Establish and maintain a Problem Management knowledgebase (Service Portal) that is accessible to County where information about Problems, Root Cause, Known Errors, Workarounds and problem resolution actions will reside.	X	
8. Provide unrestricted access by County-authorized staff and other County designated personnel to all current and historical Problem Management records and knowledgebase data.	X	
9. Ensure Problem Management activities conform to defined Change Management procedures set forth in the Procedures Manual.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
10. Coordinate with appropriate Incident Management teams and take ownership of Problem Management activities of all problems determined to reside in the Frameworks.	X	
11. Coordinate, escalate and track Problem Management activities within County and Third-Parties related to problems determined to reside in all infrastructure areas.	X	
12. Flag all Incidents that require further RCA to be conducted (i.e., Severity 1 and Severity 2 Incidents) per the agreed-to procedures.	X	
13. Ensure that recurring problems that meet defined criteria related to the Contractor's service responsibility area are reviewed using RCA procedures.	X	
14. Conduct proactive trend analysis of Incidents and problems, and other data elements to identify recurring situations that are or have the potential to be indicative of future problems and points of failure.	X	
15. Track and report on problems and trends or failures and identify associated consequences of problems.	X	
16. Develop and recommend corrective actions or solutions to address recurring Incidents and problems, as well as mitigation strategies and actions to take to avert potential problems identified through trend analysis.	X	

Problem Management Services Roles and Responsibilities		
17. Identify, develop, document, and recommend appropriate Workarounds for known errors of unresolved problems and notify Incident Management and all other appropriate stakeholders of its availability if approved. Document the workaround in the knowledgebase.	X	
18. Review and approve Workarounds for implementation, as appropriate.		X
19. Coordinate and monitor status of root-cause analysis activities performed by County and Third-Party.	X	
20. Document and update Problem Management knowledgebase with information regarding problem resolution actions, activities and status (e.g., root cause, known errors, workarounds, etc.) and notify all appropriate stakeholders of availability of information.	X	
21. Coordinate with County and Third-Party service to ensure that knowledge on Problems related to Frameworks is captured and entered into a centralized Problem Management knowledgebase.	X	
22. Ensure problem resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual.	X	
23. Provide status reports detailing the root cause and procedure for correcting recurring Problems and Severity 1 and Severity 2 Incidents until closure as determined by County.	X	
24. Conduct Problem Management review meetings and provide listing and status of same categorized by problem impact.	X	
25. Participate in Problem Management review meetings and review and approve recommendations for actions, where appropriate.		X
26. Periodically review the state of open Incidents and related problems and the progress being made in addressing Problems.	X	
27. Participate in and review and approve as appropriate all Problem Management generated Request for Change (RFCs) as part of the Change Management.		X
28. Create Request for Change (RFC) documentation with recommended corrective actions to be taken to resolve a problem and submit to County for review and approval.	X	
29. Conduct periodic problem management proactive review sessions.	X	

Problem Management Services Roles and Responsibilities		
30. Provide Problem Management reporting on a weekly basis for all activity.	X	

2.13. Change Management Services

2.13.1. Overview

Change Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with standardized methods and procedures that are used for efficient and prompt handling of all changes. Change Management Service apply to all changes across all Frameworks, and minimize the impact of any change to the quality and operation of the Services.

The Change Management processes and activities are inter-related and complementary with Release Management and Configuration Management, as well as Incident Management and Problem Management.

2.13.2. High Level Requirements

2.13.2.1. Contractor shall develop, deliver (for County approval), post to Service Portal and continuously maintain standardized methods and procedures for Change Management Services.

2.13.2.2. Contractor shall develop process for handling Hardware and Software version control through Change Management Services.

2.13.2.3. Contractor shall establish a centralized control point for Change Management Services.

2.13.2.4. Contractor shall ensure minimal conflict and potential service disruption for all changes.

2.13.2.5. Contractor shall eliminate and prevent all unauthorized changes to the Services.

2.13.2.6. Contractor shall implement maintenance windows for changes affecting the Services.

2.13.2.7. Contractor shall minimize the amount of emergency changes to the Services.

2.13.2.8. Contractor shall record all changes made to the Services.

2.13.2.9. Contractor shall ensure all changes are evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner with County participation.

2.13.2.10. Contractor shall post on the Service Portal all documentation, changes requests, approvals, or any other information related to the Change Management Services.

2.13.2.11. Contractor shall determine metrics for measuring effectiveness of a changes and will post monthly report on the Service Portal.

2.13.2.12. Contractor will coordinate and manage, with County participation, the Change Advisory Board (CAB).

2.13.2.13. Contractor shall ensure County approval is received for all changes are deemed approved.

2.13.2.14. Contractor shall establish and manage the schedule of approved changes Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.13.2.15. Contractor shall annually update and deliver the Change Management Services Management plan, for County approval, and posted on the Service Portal.

2.13.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Change Management Services.

Change Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Change Management Services Roles and Responsibilities		
1. Define Change Management policies and requirements, including change priority schema and classifications, per the Change Management process components outlined above.		X
2. Develop Change Management procedures, communications venues and processes per the Change Management process components outlined above.	X	
3. Participate in the development of the Change Management and CAB procedures, policies, communications venues and approval authorities.		X
4. Review and Approve Change Management process, procedures and policies.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Develop operational policies standards and procedures manual for Change Management.	X	
6. Oversee the approved change build, test, change communication and implementation processes to ensure these activities are appropriately resourced and completed according to change schedule.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Receive and document all Requests for Change (RFC) and classify proposed changes to the Services.	X	
8. Review and validate that RFCs comply with Change Management policies, procedures, and processes.		X
9. Ensure that appropriate back-out plans are documented and in place in the event of systems failure as a result of the change.	X	
10. Provide Change Management plan to County for review.	X	
11. Review and approve Change Management plan.		X
12. Recommend change management communication venues.	X	
13. Review and approve change management communication venues.		X
14. Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes or FSC) for County to review.	X	

Change Management Services Roles and Responsibilities		
15. Coordinate, schedule, and conduct Change Advisory Board (CAB) meetings to include review of planned changes and results of changes made, ensuring that all appropriate parties are invited and represented in accordance with approved CAB policies.	X	
16. Provide change documentation as required, including proposed metrics as to how effectiveness of the change to be measured.	X	
17. Review and approve change documentation and change effectiveness metrics.		X
18. Review and approve any RFC determined to have significant risk impact to the Services.		X
19. Authorize and approve scheduled changes or alter the schedule change requests as defined in the Change Management procedures.		X
20. Publish and communicate the approved FSC to all appropriate IT and Business Group stakeholders within County of change timing and impact.		X
21. Participate in business risk assessment for change to be introduced without being fully tested.	X	
22. Monitor changes, perform change reviews and report results of changes, impacts, and change effectiveness metrics.	X	
23. Verify that change met objectives based upon predetermined effectiveness metrics and determine follow-up actions to resolve situations where the change failed to meet objects.	X	
24. Review and approve change management results.		X
25. Close out RFCs that met the change objectives or changes that were abandoned.	X	
26. Perform Change Management quality control reviews and reviews of Change Management processes, and records.		X
27. Provide County Change Management reports as required and defined by County.	X	

2.14. Release Management Services

2.14.1. Overview

Release Management Services Framework Component of Cross Functional Services are the roles and responsibilities that are concerned with implementing approved changes to the Services. Release Management Services are activities that take a holistic view of scheduled changes to the Services and ensure that the technical and non-technical dependencies of the release. Release Management Service encompasses the planning, design, build, configuration and testing of hardware and software releases to create a defined set of release policies and procedures.

The Release Management processes and activities are inter-related and complementary with Change Management and Configuration Management, as well as Incident Management and Problem Management.

2.14.2. High Level Requirements

2.14.2.1. Contractor shall establish standardized Release Management policies and procedures, for County approval, and post to the Service Portal.

2.14.2.2. Contractor shall manage the release plans and schedules for approved changes.

2.14.2.3. Contractor shall develop, deliver and continuously manage release documentation.

2.14.2.4. Contractor shall develop, deliver, and continuously manage the release design, build, and configuration processes.

2.14.2.5. Contractor shall implement release testing, if appropriate, for all approved changes.

2.14.2.6. Contractor shall document, deliver and post on the Service Portal rollout planning including quality plans and back-out plans for releases.

2.14.2.7. Contractor shall document, deliver and post on the Service Portal all release communication, preparation, and training.

2.14.2.8. Contractor shall manage the rollout/distribution and installation of all elements of a release.

2.14.2.9. Contractor shall document each release and shall update the Configuration Management Database (CMDB).

2.14.2.10. Contractor shall annually update and deliver the Release Management Services Management plan, for County approval, and posted on the Service Portal.

2.14.3. Environment

2.14.3.1. Releases

Releases consist of a number of corrective action fixes and enhancements to the Services. A Release consists of the new or changed software required and any new or changed Hardware needed to implement the approved changes. Categories of releases are below:

- Major Software releases and Hardware upgrades or replacements, normally containing large areas of new functionality. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes
- Minor Software releases and Hardware upgrades, normally containing small enhancements and fixes. A minor upgrade or release usually supersedes all preceding emergency fixes
- Emergency Software and Hardware fixes, normally containing the corrections to a small number of known Incidents

2.14.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Release Management Services.

Release Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Release Management policies and requirements per the Release Management process components outlined above.		X
2. Develop Release Management procedures and processes per the Release Management process components outlined above.	X	
3. Participate in the development of the Release Management process and procedures and policies.		X
4. Review and approve Release Management process procedures and policies.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Develop operational policies standards and procedures manual for Release Management.	X	
6. Establish and maintain an appropriate secure environment(s) where all authorized versions of all Software, in physical or electronic form as applicable (Definitive Software Library or DSL) and where all hardware spares (Definitive Hardware Store or DHS) are stored, protected and accounted.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Maintain master copies of all new versions of Software (both COTS Software packages and application developed custom-built Software) in the secured DSL and update configuration item.	X	
8. Ensure that all hardware spares are secured in the DHS and reflected in the configuration management database(s).	X	
9. Establish, manage, update, and maintain the overall Release Plan and Release Schedule for all planned Releases.	X	
10. Establish and administer the version control schema as it relates to Release Management of County custom applications.	X	
11. Develop, manage, update and maintain formal Release Plans for each Release in coordination with Change Management.	X	
12. Develop quality plans and back-out plans as appropriate for each Release.	X	
13. Provide Release Management Plans and Schedules to County for review.	X	
14. Review and approve Release Management Plans and Schedules.		X

Release Management Services Roles and Responsibilities		
15. Conduct site surveys, as necessary, to assess existing Hardware and Software being used to validate Release package requirements and dependencies.	X	
16. Plan resource levels and requirements for supporting a release.	X	
17. Ensure that any new Software, Hardware, or support services required for the release are procured and available when needed.	X	
18. Ensure that all necessary testing environments are available and properly configured to support Release testing.	X	
19. Ensure there is segregation of duties between the application developer testers and the release management testers.	X	
20. Conduct post-deployment testing as required.	X	
21. Schedule and conduct Release Management meetings to include review of planned releases and results of changes made.	X	
22. Identify and document all Configurable Items (CIs) that need to be included in the Release, as well as all system inter-dependencies.	X	
23. Plan and manage the acceptance testing process for each Release.	X	
24. Review and approve Release acceptance testing plans.		X
25. Provide Release documentation as required.	X	
26. Authorize and approve scheduled Releases or alter the schedule as defined in the Release Management procedures.		X
27. Review Release Management details and alter as appropriate to meet the needs of the County (e.g., back out plan, go/no go decision).	X	
28. Notify County of Release timing and impact and provide communications to the Service Desk.	X	
29. Implement Release in compliance with Change Management requirements and adherence to detailed release plans.	X	
30. Modify configuration database, Asset Management items, and service catalog (if applicable) to reflect changes to CIs due to the Release.	X	

Release Management Services Roles and Responsibilities		
31. Conduct post-mortem of Releases that necessitated implementation of the back out plan and develop and implement appropriate corrective or follow-up actions to minimize future occurrences.	X	
32. Perform quality control reviews and approve Release control results.		X
33. Provide County Release Management reports as required and defined by County.	X	

2.15. Configuration Management Services

2.15.1. Overview

Configuration Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with the recording, tracking, updating and disseminating the County's configurations for all Assets. Configuration Management Services will provide an integrated Configuration Management Database (CMDB), will capture all logical configurations of Hardware and Software supporting the Services, contain mappings to physical configuration, inventory data of Hardware and Software, analyze trends and be used to manage and reduce Incidents and Problems.

The Configuration Management processes and activities are inter-related and complementary with Change Management and Release Management, as well as Incident Management and Problem Management.

2.15.2. High Level Requirements

2.15.2.1. Contractor shall deliver and maintain an integrated Configuration Management Database (CMDB).

2.15.2.2. Contractor shall make available the CMDB through the Service Portal for approved County End-Users.

2.15.2.3. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and processes related to Configuration Management Services.

2.15.2.4. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Configuration Management methodology.

2.15.2.5. Contractor shall own Configuration Management end-to-end.

2.15.2.6. Contractor shall monitor, optimize, maintain, document, and report on all County Hardware and Software configurations, including but not limited to new releases and versions, patches, and bug fixes.

2.15.2.7. Contractor shall update the CMDB promptly after the completion of any approved change or release.

2.15.2.8. Contractor shall identify configuration items, control and manage changes to configuration items, provide status accounting of those changes, verify functional and physical characteristics of configuration items, release and deliver configuration items.

2.15.2.9. Contractor shall perform configuration identification, control, status accounting, reviews and release management according to County policies and procedures.

2.15.2.10. Contractor shall use a tool set or suite of tools to ensure application configuration and code management is securely stored, managed and accessible as the system of record for configuration management and code management.

2.15.2.11. Contractor shall provide an enterprise code version manager to be the central repository for Portfolio Application configurations, patch downloads, software downloads, custom code, scripts and any software asset required to maintain or restore Portfolio Applications.

2.15.2.12. Contractor shall support, maintain and manage the enterprise code version manager including updates to ensure functionality and currency for code release, code deployment and accessibility.

2.15.2.13. Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.15.2.14. Contractor shall annually update and deliver the Configuration Management Services Management plan, for County approval, and posted on the Service Portal.

2.15.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Configuration Management Services.

Configuration Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit configuration management policies, procedures and policies.	X	
2. Review and approve configuration management policies, procedures and standards.		X
3. Produce and submit recommendations for configuration changes.	X	
4. Review and approve configuration changes.		X
5. Establish and maintain a single approach to manage both the County Configuration Management Database (referred to as the Unified Configuration Management Database) and the Integrated Asset Management System in accordance with the County's requirements.	X	
6. Monitor Third-Party announcements regarding software upgrades, patches, reported Incidents and published solutions.	X	
7. Provide impact analysis and propose installation plans for announced fixes.	X	
8. Recommend the applications packages that can be regularly reviewed for patches or version release upgrades and review this list per a defined schedule.	X	

Configuration Management Services Roles and Responsibilities		
9. Identify and report when patches or version-release upgrades are available for Applications and determine which functionalities are newly available as a result of the upgrade or which system Incidents are addressed by it, particularly when this improves customer ease of use.	X	
10. Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes.	X	
11. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing.	X	
12. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items.		X
13. Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states.	X	
14. Develop procedures for establishing security baselines as reference points for rebuilds, and provide ability to revert to stable configuration states.		X
15. Establish procedures for verifying the accuracy of configuration items, adherence to Configuration Management process and identifying process deficiencies.	X	
Build Roles and Responsibilities	**Contractor**	**County**
16. Implement and maintain configuration management policies and procedures.	X	
17. Establish a Change and Release Control Board (CRCB) that approve CM policies and their inclusion in Standards and Procedures in the County Standards and Procedures Manual, and shall approve or delegate approval of changes and releases of updates.	X	
18. Provide the County Standards and Procedures Manual for CRCB for County Approval.	X	
19. Approve the County Standards and Procedures Manual for CRCB.		X
20. Participate in Change and Release Control Board (CRCB) and review and approve CRCB activities and decisions.		X

Configuration Management Services Roles and Responsibilities		
21. Select, install and maintain configuration management tools.	X	
22. Ensure and follow change control and notification processes for installations, upgrades and adjustments to components, software and County processes.	X	
23. Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing.	X	
24. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and regressing of configuration items.	X	
25. Establish configuration baselines as reference points for rebuilds, and providing ability to revert to stable configuration states.	X	
26. Establish process for verifying the accuracy of configuration items; adherence to configuration standards, management process and the identification of process deficiencies.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Perform configuration management.	X	
28. Identify when configuration item changes or updates affect other services.	X	
29. Install manufacturer field change orders, service packs, firmware, and software maintenance releases, etc.	X	
30. Perform configuration management activities throughout the system life-cycle.	X	
31. Perform configuration management activities throughout the development life cycle.	X	
32. Perform configuration management and change management activities related to integration and testing.	X	
33. Perform product patch, “bug fix,” service pack installation or upgrades to the current installed version.	X	
34. Review configuration management results and accuracy of configuration data.		X
35. Correct any inaccurate configuration data and CIs.	X	

Configuration Management Services Roles and Responsibilities		
36. Maintain master copies of new versions in a secured software library and update configuration databases.	X	
37. Administer the version control system as it relates to release management of County Applications.	X	
38. Ensure that inventory and configuration management records are maintained and that all updates to County and Contractor records are reflected.	X	
39. Provide document version control for all documentation for which Contractor is responsible.	X	
40. Inform the County of changes through the weekly change and release control meetings and periodic integrated change status reporting. Each change request shall identify other related change requests to facilitate integrated reporting.	X	

2.16. Capacity Planning and Performance Management Services

2.16.1. Overview

Capacity Planning and Performance Management Services Framework Component of Cross Functional Services are the roles and responsibilities that support activities associated with optimizing the efficiency, effectiveness, capacity and technical performance of the Hardware and Software performing the Services. Capacity Planning and Performance Management Services will provide process of determining the resources required, will prevent performance or availability impact to County business, develop and manage services response time and quality of services for End-Users.

The Capacity Planning and Performance Management processes and activities are inter-related and complementary with Change Management and Release Management, as well as Incident Management and Problem Management.

2.16.2. High Level Requirements

2.16.2.1. Contractor shall monitor and manage systems to leverage and optimize the Services.

2.16.2.2. Contractor shall develop, deliver (for County approval), post on the Service Portal and continuously maintain all procedures and

processes related to Capacity Planning and Performance Management Services.

2.16.2.3. Contractor shall develop, deliver, post on the Service Portal and continuously maintain the Capacity Planning and Performance Management methodology.

2.16.2.4. Contractor shall own Capacity Planning and Performance Management end-to-end and across all Service Frameworks.

2.16.2.5. Contractor shall analyze historical resource usage by tracking and trending Hardware and Software performing the Services.

2.16.2.6. Contractor shall continuously perform capacity analysis across the Hardware and Software performing the Services.

2.16.2.7. Contractor shall develop, deliver (for County approval) and implement a capacity plan on an annual basis for Hardware and Software performing the Services.

2.16.2.8. Contractor shall develop, deliver (for County approval), and implement a on a monthly basis a list of tuning activities for Hardware and Software performing the Services.

2.16.2.9. Contractor shall continuously monitor, measure, forecast and post to the Service Portal capacity actuals, historical resource use trends and corrective actions on a monthly basis.

2.16.2.10. Contractor shall model short-term and long-term resource usage and performance based on proposed approved releases.

2.16.2.11. Contractor shall identify and implement improvements to better leverage existing capacity.

2.16.2.12. Contractor shall communicate potential capacity or performance Incidents to the County in advance, and implement approved solutions in a timely manner.

2.16.2.13. Contractor shall annually update and deliver the Capacity and Performance Management Services Management plan, for County approval, and posted on the Service Portal.

2.16.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Capacity Planning and Performance Management Services.

Capacity Planning and Performance Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Conduct capacity planning activities that incorporate all Systems, sub-systems, and software, workload balancing, and resource allocation.	X	
2. Develop or provide tools to monitor capacity and performance.	X	
3. Review and approve tools to monitor capacity and performance.		X
4. Recommend changes to capacity to improve service performance.	X	
5. Approve capacity-related recommendations.		X
6. Produce and submit recommendations for changes to optimize capacity management.	X	
7. Review and approve changes to optimize capacity management.	X	
8. Produce and submit projections prior to the start of each contract year regarding estimated usage and loading for all Service Frameworks based on historical trends, anticipated new projects and decommissioning of systems, etc.	X	
9. Develop and maintain a capacity plan to meet the County's existing and future needs. The process components of the capacity Management plan shall include: • Application sizing • Resource forecasting • Demand forecasting • Modeling • Performance monitoring • Workload monitoring	X	
10. Perform Application capacity and performance planning by incorporating business projections provided by the County.	X	

Capacity Planning and Performance Management Services Roles and Responsibilities		
11. Perform capacity and performance planning on an ongoing basis when new business and application growth is anticipated, when changes to existing business requirements are anticipated or occur, or when system configuration changes are performed.	X	
Build Roles and Responsibilities	**Contractor**	**County**
12. Implement comprehensive capacity management planning process as well as tools to monitor capacity and performance.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
13. Maintain capacity levels to optimize use of existing resources and minimize County costs to deliver Services in accordance with the Service Levels.	X	
14. Monitor and manage capacity in all Service Frameworks to maximize performance and efficiency and to minimize service disruptions.	X	
15. Assess impact/risk and cost of capacity changes and submit mitigation recommendations.	X	
16. Continually monitor resource usage to enable proactive identification of capacity and performance Incidents.	X	
17. Capture trending information and forecast future County capacity requirements based on County defined thresholds.	X	
18. Assess capacity impacts when adding, removing or modifying Applications.	X	
19. Assess Incidents/Problems related to throughput performance.	X	
20. Recommend and perform approved DBMS tuning changes.	X	
21. Conduct periodic database reorganizations as indicated by usage and performance.	X	
22. Define and execute database performance and tuning scripts and keep database running at optimal performance for County's workload.	X	
23. Implement and administer appropriate database management tools across all database instances.	X	
24. Validate asset utilization and capacity efficiency.	X	
25. Participate in all capacity planning activities.		X

Capacity Planning and Performance Management Services Roles and Responsibilities		
26. Perform Framework Component tuning to maintain optimum performance in accordance with Change Management procedures.	X	

2.17. Disaster Recovery Management Services

2.17.1. Overview

The Disaster Recovery (DR) Framework Component within the Cross Functional Framework applies to the process for resumption of County business after a disruptive event. Disaster Recovery Management Services will provide strategy, process, type, methodology, locations, documentation and prompt restoration of the Services.

Disaster Recovery Management Services planned and implemented as part of the Data Center Framework. Types of DR to consider would be:

- Active/Active – synchronous
- Active/Passive – asynchronous
- Active/Passive – vault

Contractor shall propose a plan, during transition, to execute for Disaster Recovery Services. The plan should consider the following:

- Portfolio Applications priorities and RTO/RPO requirements
- Active/Active-synchronous methodology
- Active/Passive – asynchronous methodology
- Active/Passive – vault methodology
- Data Synchronization and replication plans
- Reduce licensing costs
- Validation that restoration times meet the requirement of the Service Levels

2.17.2. High Level Requirements

2.17.2.1. Contractor shall develop the type of DR that will be used to support the Services.

2.17.2.2. Contractor shall execute the DR plan upon County declaration of a disruptive event.

2.17.2.3. Contractor shall recover and resume full operations of Severity 1 applications, including all supporting infrastructure and network within 48 hours.

2.17.2.4. Contractor shall recover and resume full operations of Severity 2 applications, including all supporting infrastructure and network within 72 hours.

2.17.2.5. Contractor shall recover all County Data repositories with a data loss of no greater than 28 hours.

2.17.2.6. Contractor shall provide, for County approval, the initial and executable DR plan during the Transition period.

2.17.2.7. Contractor shall submit, for County approval, annual updates to the DR plan.

2.17.2.8. Contractor shall review the County's Business Continuity Plans and use in the development of the DR plan.

2.17.2.9. Contractor shall ensure the DR plan covers all the Service Frameworks.

2.17.2.10. Contactor shall adjust the DR plan with new items that the County, in writing, deems necessary.

2.17.2.11. Contractor shall implement the full DR plan prior to the conclusion of Transition.

2.17.2.12. Contractor shall implement changes, if any, within three (3) months related to the County approved annual DR plan.

2.17.2.13. Contractor shall update the DR plan based on technology related environmental changes and updates.

2.17.2.14. Contractor shall create, update and maintain working procedures for execution of the DR plan in the Standards and Procedures Manual.

2.17.2.15. Contractor shall perform an annual test of the DR plan.

2.17.2.16. Contractor shall provide a full report, for County approval, of the DR plan annual test.

2.17.2.17. Contractor shall correct any discrepancies discovered in the annual DR test within three (3) months Contractor shall develop and deliver a management plan, for County approval, during Transition and posted on the Service Portal.

2.17.2.18. Contractor shall annually update and deliver the Disaster Recovery Management Services Management plan, for County approval, and posted on the Service Portal.

2.17.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with DR Management Services.

DR Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a DR plans that meets County requirements.	X	
2. Review and approve the DR plan that meets County requirements.		X
3. Produce and submit data recovery plan consistent with the County's business requirements.	X	
4. Review and approve data recovery plan.		X
5. Produce and submit at the start of each Contract Year a revised DR Plan to continually meet County objectives.	X	
6. Review and approve the yearly DR Plan.		X
7. Produce and submit a yearly DR test plan.	X	
8. Approve the DR test.		X
9. On an annual basis, review the prioritization of application portfolio and reclassify, if required, priority levels.	X	
10. Designate the criticality recovery level for each application in the County application portfolio.	X	

DR Management Services Roles and Responsibilities		
11. Review and approve the assigned criticality levels.		X
Build Roles and Responsibilities	**Contractor**	**County**
12. Design and implement DR plan.	X	
13. Design and implement data recovery plan.	X	
14. Coordinate the DR plans with the County Technology Office plans to address any potential disconnects or misunderstanding.	X	
15. Submit yearly DR test Plans to the County.	X	
16. Perform yearly DR test.	X	
17. Submit yearly DR test results to the County.	X	
18. Review and approve yearly DR test results.		X
19. Maintain and document requirements for off-site data storage.	X	
20. Review documentation for off-site data storage.		X
Operate Roles and Responsibilities	**Contractor**	**County**
21. Provide secure offsite storage for designated media and transport media to offsite location as required (include handling, storing, shipping, and receiving media).	X	
22. Ensure archived data is available for use in disaster recovery operations.	X	
23. Provide off-site backup media storage.	X	
24. Establish and maintain contracts for hot-site or cold-site availability as required, coordinate disaster recovery exercises to ensure readiness, and perform required recovery.	X	
25. Promote DR by meeting with the County's CIO, governance committees, the business managers, and the departments to provide appropriate communication during any DR operation.	X	
26. Perform scheduled DR tests per County policies, requirements and the DR Plan.	X	
27. Track and report DR test results to the County.	X	
28. Approve DR testing results.		X
29. Perform corrective action identified during the DR test and provide ongoing status until completion.	X	

DR Management Services Roles and Responsibilities		
30. Provide a written DR test and corrective action report to the County by a mutually agreed upon date each year.	X	
31. Execute DR Procedures when directed by an authorized representative of the County.	X	
32. Provide DR recovery within Service Levels from the time a disaster is declared for Priority 1 Applications.	X	
33. Provide DR recovery within the Service Levels from the time a disaster is declared for Priority 2 Applications.	X	
34. Provide DR recovery within the specified Service Levels from the time a disaster is declared for all required Applications to support Priority 1 and 2 Applications.	X	

2.18. Identity Access Management Services

2.18.1. Overview

Identity Access Management (IAM) Services Framework Component of the Cross Functional Framework applies to the business processes that facilitates the management of electronic identities. The IAM Framework Component includes all the technology, services and support needed to support identity management.

2.18.2. High Level Requirements

2.18.2.1. Contractor shall submit, for County approval, and implement an executable IAM plan to consolidate County identities into a single, federated IAM solution.

2.18.2.2. Contractor shall federate and maintain identities into the IAM solution per County Service Request.

2.18.2.3. Contractor shall provide, for County approval, the initial and executable IAM plan during the Transition period.

2.18.2.4. Contractor shall participate in architecture and strategy sessions with the County to determine and maintain the IAM roadmap.

2.18.2.5. Contractor shall develop automated workflow to manage access Service Requests.

2.18.2.6. Contractor shall implement automation tool for IAM to initiate, capture, record and manage End-User identities and their related access permission.

2.18.2.7. Contractor shall follow County policy in the provision of IAM Services

2.18.2.8. Contractor shall ensure that the IAM solution is reviewable and in compliance with any applicable regulatory process.

2.18.2.9. Contractor shall ensure the maintenance of overall security for the IAM solution.

2.18.2.10. Contractor shall track, maintain and review End-Users access privileges who migrate to different jobs within the County.

2.18.2.11. Contractor shall implement IAM with a centralized directory service that is scalable.

2.18.2.12. Contractor shall implement IAM to facilitate the process of user provisioning and account setup with a controlled and automated workflow.

2.18.2.13. Contractor shall provide monthly reporting on all changes to the IAM repository.

2.18.2.14. Contractor shall retain all Service Requests for IAM Services that can be used for review and reporting.

2.18.2.15. Contractor shall provide automated interface to County PeopleSoft application for employee IAM Services.

2.18.2.16. Contractor shall identify and manage non-County users distinctly from County employees.

2.18.2.17. Contractor shall provide attestation functionality to be used for identity management.

2.18.2.18. Contractor shall implement and maintain synchronization of all non-IAM End-User accounts across disparate applications or cloud-based services.

2.18.2.19. Contractor will continuously consolidate disparate End-User accounts into IAM.

2.18.2.20. Contractor shall implement IAM as the single solution for all County identity services.

2.18.2.21. Contractor shall provide the capability for Portfolio Applications to integrate and use the enterprise single sign-on.

2.18.2.22. Contractor shall maintain the Service Desk for all End-User IAM related Service Requests.

2.18.2.23. Contractor shall annually update and deliver the Identity Access Management Services Management plan, for County approval, and posted on the Service Portal.

2.18.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Identity Access Management Services.

Identity Access Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommended processes for Identity Access Management authentication and authorization.	X	
2. Review and approve processes for Identity Access Management authentication and authorization.		X
3. Produce and submit escalation procedures for quick termination.	X	
4. Review and approve escalation procedures for quick termination.		X

Identity Access Management Services Roles and Responsibilities		
5. Produce and submit End-User Identity Access Management architecture.	X	
6. Establish and manage process to support temporary access.	X	
7. Review and approve End-User Identity Access Management architecture.		X
8. Produce and submit annual End-User account consolidation plan.	X	
9. Review and approve annual End-User account consolidation plan.		X
10. Produce and submit the format for a report detailing all County End-User accounts and End-User data permissions.	X	
11. Review and approve the format for a report detailing all County End-User accounts and End-User data permissions.		X
12. Develop a service ordering process that clearly defines how to order change or delete services.	X	
13. Define logging and archiving policies and requirements.		X
Build Roles and Responsibilities	**Contractor**	**County**
14. Implement systems to centrally manage and maintain Account Management data and activities.	X	
15. Implement approved processes for Identity, Access and Account Management authentication and authorization.	X	
16. Implement reports detailing all County End-User accounts and End-User data permissions.	X	
17. Implement End-User account consolidation plan.	X	
18. Analyze account management architecture and the access control systems of the County's business applications, and develop and implement an End-User Account Consolidation Plan and End-User Identity, Access and Account Management architecture that provides a platform for account synchronization across the enterprise and across disparate systems.	X	
19. Implement End-User Account Management architecture.	X	
20. Implement escalation procedures for quick termination.	X	
21. Provide logging and archiving specifications/design.	X	

Identity Access Management Services Roles and Responsibilities		
22. Approve logging and archiving specification/design.		X
Operate Roles and Responsibilities	**Contractor**	**County**
23. Centrally maintain End-User accounts.	X	
24. Perform End-User account maintenance to include account creation, deletion or modification.	X	
25. Perform End-User account password resets.	X	
26. Perform End-User authorized data permission requests.	X	
27. Facilitate the receipt and tracking of requests for End-User account activation, changes and terminations.	X	
28. Facilitate the creation, change and deletion of End-User accounts.	X	
29. Coordinate as necessary with other specialized areas to manage End-User accounts.	X	
30. Maintain Access Control Lists (ACL) in accordance with policies.	X	
31. Provide report detailing all County End-User accounts and End-User data permissions on a monthly basis.	X	
32. Provide, update and maintain a reviewable record of security modifications and produce reports and notifications of End-User access modifications, transfers, and terminations.	X	
33. Provide support, including break-fix, for all Identity, Access and Account Management Services.	X	
34. On an annual basis, update the End-User Account Consolidation Plan to reflect progress toward reduction of User IDs and credentials, and to make recommendations for implementation of new technologies within the Identity, Access and Account Management architecture.	X	
35. Support and maintain Identity, Access and Account Management technology solution for infrastructure.	X	
36. Perform engineering, configuration and ongoing management of Identity, Access and Account Management technology solution.	X	
37. Log and archive User/account activity according to approved logging and archiving specification/design.	X	

Identity Access Management Services Roles and Responsibilities		
38. Periodically review production system access logs and activities to identify malicious or abnormal behavior in accordance with established County policies and standards.	X	
39. Periodically review all County account IDs to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established County policies and standards.		X
40. Periodically review all privileged User accounts to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established County policies and standards.	X	
41. Periodically review End-User accounts to ensure each User has appropriate minimal permissions required to perform their job function in accordance with established County policies and standards.	X	
42. Periodically review privileged User accounts to ensure each User has appropriate minimal permissions required to perform their job function in accordance with established County policies and standards.	X	

2.19. Reporting Management Services

2.19.1. Overview

Reporting Management Services Framework Component of the Cross Functional Framework applies to the activities associated with the development, generation and submission of deliverables defined in Schedule 5 of the Agreement.

In addition, Contractor shall report system management information (e.g., performance metrics, and System accounting information) to the County in an on-line dashboard and electronic reports.

2.19.2. High Level Requirements

2.19.2.1. Contractor shall provide accurate and timely reporting on performance, trends, Incidents, Assets, and other topics as required by the County.

2.19.2.2. Contractor shall provide, for County approval, the initial and executable Reporting Management Services Management Plan during the Transition period.

2.19.2.3. Contractor shall ensure Reporting Management Services is fully implement prior to the end of Transition.

2.19.2.4. Contractor shall update and maintain the Reporting Management Services Management Plan on an annual basis.

2.19.2.5. Contractor shall post the County approved, Reporting Management Services Management Plan to the Service Portal.

2.19.2.6. Contractor shall post all Schedule 5 deliverables to the Service Portal.

2.19.2.7. Contractor shall develop, with County approval, all deliverables are comprehensive and detailed.

2.19.2.8. Contractor shall maintain and provide electronic online dashboards on the Service Portal for Performance Metrics.

2.19.2.9. Contractor shall annually update and deliver the Reporting Management Services Management plan, for County approval, and posted on the Service Portal.

2.19.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Reporting Management Services.

Reporting Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define reporting requirements, format and frequency.		X
2. Assist the County to identify recurring reporting and format requirements to support the County's needs for information.	X	
3. Produce and submit Reporting operational policies and procedures based on County requirements.	X	

Reporting Management Services Roles and Responsibilities		
4. Review and approve Reporting operational policies and procedures based on County requirements.		X
5. Produce and submit recommendations for measurement and reporting of Service Levels.	X	
6. Review and approve recommendations for measurement and reporting of Service Levels.		X
7. Produce and submit required County reports.	X	
8. Review and approve required County reports.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Design and implement required County reports.	X	
10. Design and implement approved recommendations for measurement and reporting of Service Levels.	X	
11. Review and approve Service Level monitoring and Reporting procedures.		X
12. Implement Reporting operational policies and procedures.	X	
13. Design an automated notification system that periodically reminds the report owner of upcoming submission dates.	X	
14. Review and approve an automated notification system that periodically reminds the report owner of upcoming submission dates.		X
15. Implement the approved automated notification system that periodically reminds the report owner of upcoming submission dates. A summary of reports due within 30, 60, and 90 days must be provided.	X	
16. Design and implement a secure Service Portal that provides the County access to web-based, self-service, customer displays of key IT metrics in a dashboard view.	X	
17. Review and approve design for a secure Service Portal that provides the County access to web-based, self-service, personalized customer displays of key IT metrics in a dashboard view.		X
18. Design and implement an automated data collection and reporting system that supports the County of San Diego's yearly budgeting process, and give the County insight into the cost details of yearly operations.	X	

Reporting Management Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
19. Produce and submit all reports and other written deliverables specified in Schedule 5 or Schedule 4.3.	X	
20. Review and approve all reports and other written deliverables specified in Schedule 5 or Schedule 4.3.		X
21. Provide the County access and input to Incident and Problem tracking system to allow for Incident/Problem monitoring and ad hoc reporting.	X	
22. Provide management reports to County on the progress of the all refresh plans.	X	
23. Report on service performance improvement results.	X	
24. Provide County configuration management reports.	X	
25. Measure and Report monthly on each Service Levels.	X	
26. Report on Service Levels performance and improvement results.	X	
27. Coordinate Service Levels monitoring and reporting with designated County representative and Third-Parties.	X	
28. Measure, analyze and provide management reports on performance relative to Service Levels.	X	
29. Conduct Service Levels improvement meetings to review Service Levels and recommendation for improvements.	X	
30. Review and approve Service Levels improvement plans.		X
31. Implement Service Levels improvement plans.	X	
32. Review and approve Service Levels metrics and performance reports.		X
33. Provide the County access to performance and Service Levels reporting and monitoring system and data.	X	
34. Produce and submit monthly reporting on Applications, showing costs broken down by Plan, Build and Operate. The Operate costs needs to be broken down into the categories unscheduled maintenance, scheduled maintenance, administration, User support, and development and integration.	X	
35. Produce and submit trend information on defects, Service Requests and estimate accuracy.	X	

2.20. Domain Name Management Services

2.20.1. Overview

Domain Name Management Services Framework Component of Cross Functional Services includes the activities required to manage all County domain names in a centralized manner. The scope includes registering new domain names, maintaining the renewal schedule, reporting of all domain names, monitoring registered domain names, and insuring overall privacy of all domain names.

Domain names are unique names that identifies and organize County web services for End-Users or external users. Domain names registered with an accredited registrar provide internet based, common name translation to the actual IP address and access to the County service.

2.20.2. High Level Requirements

2.20.2.1. Contractor shall manage all domain names on behalf of the County.

2.20.2.2. Contractor shall use an accredited registrar for all domain name registrations.

2.20.2.3. Contractor shall assume ownership of all Domain Names.

2.20.2.4. Contractor shall register all domain names as requested by a Service Request.

2.20.2.5. Contractor shall comply with the County Standards and Procedures Manual for the procedure of registering, renewing and reporting of domain names.

2.20.2.6. Contractor shall not allow a domain name to expire without prior County approval.

2.20.2.7. Contractor shall notify the County POC at least 30 days in advance of the expiration date of any Domain Name.

2.20.2.8. Contractor shall annually update and deliver the Domain Name Management Services Management plan, for County approval, and posted on the Service Portal.

2.20.3. Environment

2.20.3.1. Portfolio of Domain Names

The Contractor shall maintain the Domain Names portfolio and include the following information in the Integrated Asset Management:

- Domain name ID
- Domain name
- Type / Extension
- Renewal Date
- High Org
- Low Org
- County POC Name, E-Mail and Phone
- Secondary County POC Name, E-Mail and Phone
- Registered Name Servers
- Responding Name Servers

2.20.3.2. Reports

Contractor will provide and post on the Service Portal a monthly report containing the following information:

- Total quantity of managed domain names
- Quantity of new domain names added in the last month
- Quantity of domain names transferred in the last month
- Quantity of domain names retired in the last month
- Quantity of domain names retained by the County
- Summary data for each domain name:
    - Domain name ID
    - Domain name
    - Type / Extension
    - Renewal Date
    - High Org

- Low Org
- County POC Name, E-Mail and Phone
- Secondary County POC Name, E-Mail and Phone

2.20.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Domain Name Management Services.

Domain Names Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit procedures and methodologies for managing Domain Name Management Services.	X	
2. Review and approve procedures and methodologies for managing Domain Name Management Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Implement procedures and methodologies for managing Domain Name Management Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide support, including break-fix, for all Domain Name Management Services.	X	
5. Manage and support Domain Name Management Services to meet operational and computing procedures.	X	
6. Provide and deliver monthly reports on Domain Name Management Services portfolio.	X	
7. Provide and deliver monthly notifications on renewals and expirations.	X	
8. Provide inventory reports and ensure the Integrated Asset Management sysytem contains the information for Domain Names managed by Contractor.	X	

2.21. Business Analyst Services

2.21.1. Overview

Business Analyst Services Framework Component of Cross Functional Services are the roles and responsibilities of helping County business implement technology solutions in a cost-effective manner. Business Analyst Services will provide development of business

cases, planning and monitoring, developing requirements, translating and simplifying requirements, management and communications of requirements and requirements analysis of behalf of the County business.

2.21.2. High Level Requirements

2.21.2.1. Contractor shall develop, deliver (for County approval), implement and post to the Service Portal the business analysis methodology.

2.21.2.2. Contractor shall deploy business analysts that will assist the County in transformation initiatives.

2.21.2.3. Contractor shall help County business implement technology solutions by determining requirements and communicating them effectively.

2.21.2.4. Contractor shall develop requirements management processes, tracking and reporting and documentation.

2.21.2.5. Contractor shall create Business Analyst Center that will develop relationships between Business Analysts, CTO and County business.

2.21.2.6. Contractor Business Analyst shall develop business requirements document in support of the County business engagement.

2.21.2.7. Contractor Business Analyst shall develop functional requirements in support of the County business engagement

2.21.2.8. Contractor shall annually update and deliver the Business Analyst Services Management plan, for County approval, and posted on the Service Portal.

2.21.3. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Business Analyst Services.

Business Analyst Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit procedures and methodologies for Business Analyst engagement with County.	X	
2. Review and approve procedures and methodologies for Business Analyst engagement with County.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Implement procedures and methodologies for Business Analyst engagement with County.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. [blank]		

2.22. Chief Technical Architect (CTA)

2.22.1. Overview

The Chief Technical Architect (CTA) Services Framework Component of Cross Functional Services describes the roles and responsibilities that support County business by providing fundamental technology and process structure and insights for IT and Telecommunications strategies and technology standardization and by providing visibility into infrastructure, applications, and data for County business. The CTA is designated as Key Personnel under the Agreement and will be staffed accordingly.

CTA shall provide architectural and technical leadership, oversight on all projects and develop a set of cognitive roadmaps to guide the progress of the County technology year over year.

The CTA provides the bridge between the deeply technical domain architects, business analysts and solution architects and other subject matter experts to ensure that the technology infrastructure meets enterprise goals, such as adaptability and complexity reduction.

The CTA, together with the Contractor EAA and Contractor CISO, will work directly with the CTO in the development and execution of architectural direction and strategy, develop and plan enterprise initiatives, identify and track emerging trends, identify and track internal Contractor Service catalog and changes to improve overall delivered Services, anticipate and understand transformative shifts in technology, develop and maintain

enterprise and departmental roadmaps, ability to access leveraged resource subject matter experts, maintain strong relationships with leading technology partners.

The CTA shall co-chair the CIO established Enterprise Architecture governance group with responsibilities to review all requirements documentation and designs, recommending, establishing and maintaining IT standards (e.g., Bricks), patterns, IT guiding principles, and communicating decisions to all Contractor IT staff. The CTA shall post all IT standards (bricks), patterns, and guiding principles on the Service Portal as changes occur and are approved by the Enterprise Architecture governance group. At the CIO's discretion, the core group of Enterprise Architecture governance, may consist of designated CTO staff, Contractor CTA, Contractor EAA and Contractor CISO and others as the CIO may designate.

The CTA shall have overall experience in technology architecture with an understanding of application and information architecture disciplines.

2.22.2. High Level Requirements

2.22.2.1. County shall retain authority on all matters related to overall IT Architecture.

2.22.2.2. Contractor shall recommend, for County approval, qualified CTA as Contractor Key Personnel.

2.22.2.3. Contractor CTA will work directly with CTO.

2.22.2.4. Contractor CTA will develop strategy and technical direction, approved by the County, and shall have oversight on all IT projects and Contractor support staff.

2.22.2.5. Contractor shall provide a full-time, dedicated Chief Technical Architect who shall support the County's architectural planning processes and ensure high standards of technical architecture and integration in new technology-based solutions implemented for the County.

2.22.2.6. Contractor CTA shall be responsible for executing the developed strategy including adherence to methodologies, standard processes, best practices, guiding principles, and standards.

2.22.2.7. Contractor CTA shall develop architecture planning that ties all aspects of the existing technical environment to a County business-consistent desired state.

2.22.2.8. Contractor CTA shall actively participate in all IT projects to ensure that they improve the capability and maturity of the Services.

2.22.2.9. Contractor CTA shall work directly with the EAA, the CISO and CTO to develop enterprise-wide standards and initiatives.

2.22.2.10. Contactor CTA shall develop, deliver, for County approval, all technology standards, guiding principles, patterns and design guidelines and criteria. The CTA shall continuously maintain them and post them on the Service Portal.

2.22.2.11. Contractor CTA shall co-chair, with CTO co-chair, the weekly Enterprise Architecture Governance meetings. This includes setting and tracking the agenda, documenting attendance, tracking minutes and decisions, uploading all documentation to the Service Portal, and other functions to ensure the success of the meeting.

2.22.2.12. Contractor CTA shall develop and deliver, for County approval, procedures and process for weekly Enterprise Architecture Governance meetings.

2.22.2.13. Contractor CTA shall work closely with Business Analyst Services to capture new or updated County business requirements as they are developed.

2.23. Enterprise Application Architect (EAA)

2.23.1. Overview

The Enterprise Application Architect (EAA) Services Framework Component of Cross Functional Services describes the roles and responsibilities that support County business by providing governance, review and approval of requirements, solutions, designs, technology, and architecture to integrate and optimize Portfolio Applications, interfaces and integrations across the enterprise. The EAA is designated as Key Personnel under the Agreement and will be staffed accordingly.

The EAA responsibilities include, but are not limited to: reviewing business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, align with information management strategies and overall efforts to continuously improve the provision of Services.

The EAA shall manage and promote the use of County standards, related to software applications, promote the reusability of existing services and expanded use of County platforms, serve as a subject matter expert to projects and provide support for IT project teams. The EAA provides the bridge between County business and the IT staff that ensures that the application architecture meets business goals and objectives, that promotes reusability and provides data and interface connectivity across the Enterprise.

The EAA shall have overall experience in business and application architecture disciplines with an emphasis on information architecture with an understanding of technical architecture.

2.23.1. High Level Requirements

2.23.1.1. Contractor shall recommend, for County approval, qualified Enterprise Application Architect (EAA) as Contractor Key Personnel.

2.23.1.2. Contractor EAA shall work directly with CTO.

2.23.1.3. Contractor EAA shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements.

2.23.1.4. Contractor EAA shall act as a subject matter expert on the effective use of technology in developing County business solutions.

2.23.1.5. Contractor EAA shall advise IT staff regarding the feasibility of proposed approaches to project solutions in terms of systems capabilities and established application architecture guidelines and standards.

2.23.1.6. Contractor EAA shall review all requirement documents and solution designs and recommend for approval to CTO prior to any development project actions.

2.23.1.7. Contractor EAA shall review all data and information architecture to ensure that data and interfaces are optimized for application use.

2.23.1.8. Contractor EAA shall work directly with the CTA, the CISO and County CTO to develop enterprise-wide standards and initiatives.

2.23.1.9. Contractor EAA, at CIO direction, shall be a member of the Enterprise Architecture Governance Group and will participate in all scheduled meetings.

2.23.1.10. Contractor EAA shall research and track emerging technologies and concepts for solving business problems not addressed in existing, deployed technology.

2.23.1.11. Contractor EAA shall recommend standards, guiding principles and best practices for deploying business and technology solutions.

2.23.1.12. Contractor EAA shall identify gaps between current and desired end-states and recommend solutions that close and provide greater efficiencies.

2.24. Innovation Management Services

2.24.1. Overview

The Innovation Management Services Framework Component of Cross Functional Services describes the roles and responsibilities that support the continuous innovation of County business. Innovation Management Services shall have a designated Innovation Officer as Key Personnel under the Agreement and will be staffed accordingly.

Innovation Management Services shall establish a culture and environment of progressive change throughout the term of the Agreement. The Contractor shall adopt a model of continuous innovation or transformation that allows progressive change in how the Services are delivered. This includes, but is not limited to, delivering Services via a bimodal approach, with an emphasis on exploration, agility, and speed, while still maintaining operational integrity and stability.

Innovation Management Services consist of a series of initiatives in which the Contractor will develop solutions, business case analyses, proposed pricing, possible changes to the Agreement, and project timelines and resources. The proposed initiatives will be reviewed by the Innovation Management Review Board and, if approved, shall be executed using agile and rapid-prototyping methodologies.

Innovation Management Services shall include an Innovation Management Office that will serve as the foundation for continuous business improvement, innovation, and transformation. The Innovation Office shall be the hub of a set of processes, governance, and resources to sustain innovation activities, and create a true environment of agility and high-velocity change at the County, supported by the Operational and steady-state teams.

2.24.2. High Level Requirements

2.24.2.1. Contractor shall recommend, for County approval, qualified Innovation Officer (IO), as Contractor Key Personnel.

2.24.2.2. Contractor IO shall work directly with the CTO and interface directly with County business leaders.

2.24.2.3. Contractor IO will provide recommendations to staff Innovation Management Services, with County approval, starting in Year 2 of this Agreement.

2.24.2.4. Contractor AE and CIO will chair the Innovation Management Review Board (TRB) and shall have joint approval on all proposed innovation initiatives and activities.

2.24.2.5. Contractor IO and CTO shall work with the CIO and County business to get a clear understanding of the strategy, business model and direction of the County.

2.24.2.6. Contractor IO shall develop, for County approval, charter, rules of engagement, success criteria and governance process for Innovation Management Services that shall include, but not limited to, lab environment (Dev/Ops), pilot process for rapid prototyping, joint development workshops, flexible and agile process (e.g., moving to micro services or containers), renovating existing systems (e.g., Hyperconverged infrastructure).

2.24.2.7. Contractor IO shall work with the EA function to understand the business outcomes and business capabilities the County is seeking to create.

2.24.2.8. Contractor IO shall build a collaborative cross-functional Innovation Management Services core team to help drive IT innovation and transformation; create the organizational and governance model needed to drive business innovation.

2.24.2.9. Contractor IO shall track technology innovations and trends, and identify what the opportunities are for the County.

2.24.2.10. Contractor IO shall work with the internal Contractor and County IT teams, key vendors and consultants to shape a roadmap for technology innovation.

2.24.2.11. Contractor IO shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements.

2.24.2.12. Contractor shall develop the process and governance to enable the continuation of progressive change within the County.

2.24.2.13. Contractor shall continuously look for opportunities to propose innovative and transformational initiatives.

2.24.2.14. Contractor shall perform an annual assessment of Innovation Management Services, for County review and approval.

2.24.2.15. Contractor shall identify potential impacts to the Agreement and propose recommended changes based on innovation initiatives.

3. SERVICE DESK SERVICES

3.1. Overview

This section pertains to the Service Desk Services Framework. Service Desk Services consist of Plan, Build, Operate centralized services to triage, process, track, report, and resolve End-User Incidents, Service Requests and requests for information.

The Service Desk is the single point of contact (SPOC) between End-Users and the Contractor on a day-to-day basis. The Service Desk will be the focal point for reporting, logging Incidents and Service Requests for End-Users and for providing self-help information. The Service Desk shall have a high degree of interactions with End-Users, in various forms, and shall ensure that End-Users receive all services in a timely manner, 24/7/365.

The Service Desk shall provide and maintain a Service Portal that provides communications and information to all End-Users. The Service Portal will assist End-Users in entering Service Requests, reviewing current or resolved Incidents, provide user tips and FAQs on the Services and self-service functions (i.e. password resets).

The Service Desk shall support and maintain the Service Request Management Service. The Service Request Management Service shall be the system used by End-Users for installing new services, modifying current services, moving services or removing services and acts as the primary request function tool across all Frameworks.

3.2. High Level Requirements

3.2.1. Contractor shall recommend, for County approval, qualified Service Desk Manager as Contractor Key Personnel to manage Service Desk Services.

3.2.2. Contractor shall continuously improve customer service interactions and ratings.

3.2.3. Contractor shall continuously improve Incident response time and Incidents resolution.

3.2.4. Contractor shall log, track, and resolve all Incidents and Service Requests submitted from End-Users.

3.2.5. Contractor shall continuously improve County efficiency and effectiveness by providing and utilizing knowledge databases and best practices in the areas of reporting, logging, tracking, routing, resolving and reporting of Incidents and Service Requests.

3.2.6. Contractor shall develop and deliver, for County approval, chat functionality for End-Users engaging the Service Desk.

3.2.7. Contractor shall perform a closed feedback loop process, so that the handling of Incidents that are to be incorporated into lessons learned, best practices, and appropriate solutions to improve economies, efficiencies, and performance.

3.2.8. Contractor shall ensure proficient and highly skilled Service Desk support with appropriate knowledge of the Services.

3.2.9. Contractor shall provide and post all communication of modifications to the Services on the Service Portal.

3.2.10. Contractor shall provide and post all Service Levels and Service Desk statistics in a real-time, up-to-date dashboard posted on the Service Portal.

3.2.11. Contractor shall maintain a repository for all Service Desk scripts and maintain a cycle for updates and accuracy.

3.2.12. Contractor shall create and maintain a Service Portal that allows County End-Users the following:

- Access the Service Portal from the internet and the County intranet
- Create and submit Incidents and Services Requests
- View a list of all Incidents and Services Requests
- Allow End-Users to change and reset passwords
- View an up-to-date knowledge base with solutions, tip sheets and Frequently asked Questions (FAQs)
- View Countywide announcements related to the Services
- Access all Contractor deliverables

3.3. Environment

The following further describe and scope Service Desk Services elements supported by Contractor and with which Contractor shall comply.

3.3.1. Technology Refresh

Contractor shall ensure Service Desk Services maintain technical currency and refresh of all Hardware and Software used to support the Services unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

3.4. Roles and Responsibilities

3.4.1. General Roles and Responsibilities

The following table identifies the Plan, Build and Operate Service Desk Plan roles and responsibilities that Contractor and County shall perform.

Service Desk Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Service Desk solutions that best meet County business needs and service–level requirements.	X	
2. Review and approve Service Desk solutions and Service Levels.		X
3. Perform operational planning for Service Desk capacity and performance purposes.	X	
4. Perform analysis of County environment to identify the appropriate sets of skills, training, and experience needed by Service Desk staff.	X	
5. Produce and submit operational policies and procedures including escalation.	X	
6. Review and approve operational policies and procedures.		X
7. Develop Self-Help requirements and policies with input from County.	X	
8. Review and approve Self-Help requirements and policies.		X
9. Develop, document and maintain in the Standards and Procedures Manual Self-Help Support Contractor procedures that meet County requirements and adhere to County policies.	X	

Service Desk Roles and Responsibilities		
10. Review and approve Self-Help procedures.		X
11. Develop and improve Service Desk scripts as appropriate to improve performance.	X	
12. Provide all testing services required to support Service Desk Services.	X	
13. Produce and submit all test documentation to County.	X	
14. Provide all deployment services required to support Service Desk Services.	X	
15. Produce and submit to County all deployment documentation.	X	
16. Review and approve all deployment documentation.		X
Operate Roles and Responsibilities	**Contractor**	**County**
17. Provide appropriately trained Service Desk staff.	X	
18. Identify and report all recurring Incidents.	X	
19. Implement and coordinate the RCA process on Incidents and Problems in conjunction with Incident and Problem Management process.	X	
20. Perform RCA of Incidents; document findings and take corrective actions for the Services. Resolve Problems and/or substantiate that all actions taken to prevent future reoccurrence.	X	
21. Manage all Services Requests from inception to closure (e.g., recording, troubleshooting, escalating, coordinating, resolving, reporting, closing).	X	
22. Manage Incidents end-to-end.	X	
23. Provide Service Desk Services, including provision, operation and maintenance of integrated Service Desk Systems (e.g., ACD, electronic workflow, Incident Management, self-help and self-heal, knowledge database, remote desktop control, procurement management, automated provisioning) necessary to document, track and manage Incidents and Service Requests, inquiries and Incident notifications from inception to closure across Service Frameworks using cross functional processes.	X	
24. Maintain and provide Service Desk operational policies and procedures in the Service Desk knowledge database.	X	
25. Review and approve Service Desk operational policies and procedures.		X

Service Desk Roles and Responsibilities		
26. Manage and track Incidents and Service Requests that involve multiple Service Frameworks and Third-Parties and collaborate with Third-Parties to resolution and closure.	X	
27. Provide Third-Party access to the Service Desk as required to support Incidents and Service Requests (e.g. change management, Integrated Asset Management System functions).	X	
28. Utilize Service Desk to resolve Incidents and perform Service Requests (e.g., change management, Integrated Asset Management System functions).	X	
29. Provide support for inquiries on the features, functions and usage of all Portfolio Applications and OIC items in use at County.	X	
30. Perform administration services such as creating, changing and deleting End-User desktop profiles.	X	
31. Provide Self-Help services for End-Users that includes the following, at a minimum: • Password reset tool • Service Request entry, tracking, reporting, updating and status checking	X	
32. Posting of content for current Incidents, frequently asked questions, knowledgebase, and other similar elements to the Service Portal.	X	
33. Monitor and review the effectiveness and usage to End-User self-service on the Service Portal.		X
34. Develop and provide recommendations for improvements to End-User self-service on the Service Portal.	X	
35. Review and approve recommendations for improvements to End-User self-service on the Service Portal.		X
36. Implement approved recommendations for improvements to End-User self-service on the Service Portal.	X	
37. Produce and submit proposed changes to Service Desk processes, operations and procedures.	X	
38. Review and approve proposed changes to Service Desk processes, operations and procedures.		X

Service Desk Roles and Responsibilities		
39. Conduct quality assurance reviews of Service Desk documentation for accuracy and currency annually or as requested by the County.	X	
40. Develop a priority-driven Service Request handoff process consistent with defined tiers of support.	X	
41. Review and approve priority-driven Service Request handoff process for the defined tiers of support.		X
42. Recommend Service Request and Incident Management procedures.	X	
43. Identify and describe priorities, response and resolution targets for Incidents and Service Requests that have differing impacts.		X
44. Develop, document and maintain Request and Incident Management procedures in the Service Desk operational policies and procedures.	X	
45. Review and approve Service Request and Incident Management procedures.		X
46. Select and implement Software and Hardware (e.g., IVR, ACD) needed to collect, track and manage Service Requests and Incidents received by the Service Desk.	X	
47. Verify that all requests are resolved, per the End-User, prior to closure.	X	
48. Develop and maintain a list of supported Portfolio Applications including priority level and key contacts.	X	
49. Review and approve the list of supported Portfolio Applications to handle calls and routing of Incident.		X

3.4.2. Single Point-of-Contact (SPOC) Roles and Responsibilities

Single Point of Contact (SPOC) services provide toll-free support for logging, tracking, resolution and reporting of Incidents and Service Requests for the Services.

The following table identifies any Plan, Build and Operate SPOC roles and responsibilities that Contractor and County shall perform.

Single Point-of-Contact Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Single Point-of-Contact Roles and Responsibilities		
1. Recommend SPOC procedures.	X	
2. Review and approve the SPOC procedures.		X
3. Develop, document and maintain the Service Desk knowledge database with all scripts and information needed to provide Service Desk Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide access to the Service Desk knowledge database from the Service Portal to End-Users.	X	
5. Provide SPOC call-in access via a toll-free number for the Services.	X	
6. Provide SPOC and coordination for all Incidents and requests for information and Service Requests.	X	
7. Provide multiple alternative communications channels (from the Service Portal), including voice messages, E-Mail, Internet, and chat.	X	
8. Initiate Incident management process for Severity 1-3 Incidents.	X	

3.4.3. Remote Device and Software Management Roles and Responsibilities

Remote Device and Software Management Services are the activities associated with managing, maintaining and troubleshooting Hardware and Software remotely and securely over the network to minimize the need to dispatch technical personnel on-site.

The following table identifies any Plan, Build, and Operate Remote Devices and Software Management roles and responsibilities that the Contractor and County shall perform.

Remote Device and Software Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit procedures for the Service Desk use of Remote Device and Software Management control tools.		X
2. Develop, document and maintain in the Service Desk operational policies and procedures Service Desk Remote Device and Software Management procedures that meet requirements and adhere to defined policies.	X	
3. Review and approve Remote Device and Software Management procedures.		X

Remote Device and Software Management Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
4. Each use of Remote Device and Software Management tools shall have End-User authorization.	X	
5. Diagnose Incidents using remote control tools and, when possible, implement remote corrective actions to resolve Incidents. If Resolution is not possible, escalate per the escalation procedures.	X	
6. Utilize remote controls to manage and update software, maintain configuration and inventory information, and enforce compliance standards.	X	

3.4.4. End-User Administration Services Roles and Responsibilities

End-User Administration Services are the activities associated with managing and coordinating account activation, termination, changes and expiration, and the management for End-Users.

The following table identifies any Plan, Build and Operate End-User Administration roles and responsibilities that Contractor and County shall perform.

End User Administration Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
1. Facilitate employee End-User account administration, activation, changes and terminations, including: password/account setup and reset, remote access connectivity, E-Mail accounts, End-User IDs, password resets, remote paging devices, voicemail administration, telephone lines, secure ID cards, OIC requests, etc.	X	
2. Prioritize calls to and from High Response End-Users identified in the Standards and Procedures Manual.	X	
3. Provide and maintain County escalation contact list(s).		X
4. Provide and maintain Contractor escalation contact list.	X	
5. Provide and maintain Service Desk staff access to the County Directory.	X	
6. Issue communications to Service Portal and provide status updates as required for planned and unplanned events.	X	

End User Administration Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
7. Record and maintain an up-to-date System status message that can be selected when calling the Service Desk for assistance.	X	
8. Provide End-User online status access for all requests via the Service Portal.	X	
9. Work with the Contractor operational and technical staff, as well as County, to identify solutions that minimize the need to call the Service Desk (e.g., additional End-User training, self-help opportunities).	X	
10. Approve solutions that minimize the need to call the Service Desk.		X
11. Dispatch on-site technicians as necessary.	X	
12. Categorize, prioritize and log all Incidents, Service Requests and inquiries.	X	
13. Monitor Incidents and escalate per policies and procedures until resolution.	X	
14. Diagnose and troubleshoot Incidents at the Service Desk and prior to escalation.	X	

3.4.5. IMAR (Install, Move, Add, Remove) Services Roles and Responsibilities

IMAR Services are the activities associated the end-to-end management and coordination of IMAR Service Requests including gathering the business requirements, providing authorization, logging the request, and facilitating fulfillment. All authorized IMAR requests passed automatically to the Service Desk. Examples of IMARs include, without limitation, adding Desktop Computing devices or moving network printers or a telephone handset.

The following table identifies any Plan, Build and Operate IMAR roles and responsibilities that Contractor and County shall perform.

IMAR Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit IMAR procedures for all Frameworks.	X	

IMAR Services Roles and Responsibilities		
2. Develop, document and maintain in the Service Desk operational policies and procedures the IMAR procedures.	X	
3. Review and approve IMAR procedures for all Frameworks.		X
Operate Roles and Responsibilities	**Contractor**	**County**
4. Receive and track IMAR Service Requests.	X	
5. Utilize workflow to coordinate and help perform End-User notifications and scheduling related to IMAR Service Requests.	X	
6. Confirm the requirements and scope and acquire County approval of the IMAR Service Request.	X	
7. IMAR Service Requests shall be scheduled to meet the requirements of the Service Levels.	X	
8. Approve IMAR schedule.		X
9. Coordinate approved IMAR Service Requests with Service Desk.	X	
10. Track and report status of IMAR Service Requests.	X	
11. Contact End-User to confirm completion of the IMAR Service Request.	X	
12. Verify completion of the IMAR Service Request.		X

3.4.6. Tracking and Reporting Roles and Responsibilities

The following table identifies the any Plan, Build and Operate IMAR requirements, roles and responsibilities that the Contractor and County shall perform.

Tracking and Reporting Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Annually, or as requested, recommend a list of Service Desk management reports (including standard industry KPIs).	X	
2. Review and approve updates to Service Desk management reports.		X
Operate Roles and Responsibilities	**Contractor**	**County**
3. Analyze and report on Incident trends and patterns on a monthly basis.	X	

Tracking and Reporting Roles and Responsibilities		
4. Monitor and report on Service Desk statistics and trends (e.g., Service Request volumes and trends by types of End-Users) for inclusion in the Service Portal Dashboard and Service Level reporting.	X	
5. Continuously review Incident data to detect trends, help manage high-severity Incidents and monitor training needs.	X	
6. Review report results and Service Desk operations on a monthly basis.		X
7. Provide online/access to Service Desk reports via the Service Portal.	X	
8. Track/manage/report Service Desk utilization.	X	
9. Report, monthly or sooner, repetitive Incidents, abnormal patterns of calls, and resolution recommendations.	X	
10. Review and approve recommended resolutions to the repetitive Incidents and abnormal patterns of calls.		X
11. Conduct Service Desk End-User customer satisfaction surveys on a random sample of Incidents (including both open Incidents and Incidents closed from the previous month) via an E-Mail/web-based tool.	X	
12. Provide results monthly of Service Desk End-User customer satisfaction surveys in the Service Portal.	X	
13. Produce and report on all aging Incidents and Service Requests on a monthly basis.	X	
14. Process and produce immediately tracking numbers for all reported Incidents.	X	
15. Provide reports by Enterprise, Group, Department, or Division level in the Contractor-maintained dashboard for Service Desk provided reports, statistics, and views.	X	

3.5. Service Request Management Services

3.5.1. Overview

This section pertains to the Service Request Management Services Framework Component in the Service Desk Services Framework. Service Request Management Services includes all of the services required to: enter, process, status, report Service Requests from the

County; coordinate Contractor activities to provide the Service Request; and coordinate with Third-Parties to provide the Service Request.

The Service Request Management Services is the single point tool used by End-Users to request services from the Contractor.

3.5.2. High Level Requirements

3.5.2.1. Contractor shall provide efficient and effective electronic processing of County Service Requests.

3.5.2.2. Contractor shall work with the County to develop and implement workflow policies and procedures that provide appropriate efficiency, security, and control of Service Requests.

3.5.2.3. Contractor shall coordinate its own, Subcontractor, and Third-Party resources to Service Requests.

3.5.2.4. Contractor shall provide the Service Request Management tool used to deliver the Service Request Management Services.

3.5.2.5. Contractor shall provide prompt updates to the Service Request Management tool to ensure accuracy of information presented to County End-Users.

3.5.2.6. Contractor shall provide prompt logging and routing of all Service Requests.

3.5.2.7. Contractor shall ensure that all Service Requests are accurately reported.

3.5.2.8. Contractor shall report on a monthly basis all open Service Requests.

3.5.2.9. Contractor shall process Service Requests in accordance to priorities set Standards and Procedures Manual.

3.5.2.10. Contractor shall provide solutions that meet the requirements specified by the Service Request.

3.5.2.11. Contractor shall use Service Requests to manage the workflow of all maintenance tasks and projects including the following:

- Create Service Requests to perform preventive and corrective maintenance
- Purchase parts and materials and committing inventory to a Service Requests
- Tracking the progress of a Service Requests by status
- Tracking all Service Requests costs
- Completing and closing each Service Request

3.5.2.12. Contractor shall provide access to County End-Users on the status (both current and historical) of Service Requests.

3.5.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Service Request Management Services.

Service Request Management Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Service Request operational policies and procedures.	X	
2. Review and approve recommendations for Service Request operational policies and procedures.		X
3. Produce and submit the Service Request Management Services design.	X	
4. Review and approve the Service Request Management Services design.		X
5. Produce and submit closed loop methodology for workflow entry, tracking and closing for Service Requests.	X	
6. Review and approve closed loop methodology for workflow entry, tracking and closing for Service Requests.		X

Service Request Management Roles and Responsibilities		
7. Produce and submit recommended monthly report format for Service Request.	X	
8. Review and approve monthly report format for Service Request.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Implement a closed loop processing for workflow entry, tracking and closing of the Service Requests.	X	
10. Implement the Service Request Management Services design	X	
11. Implement approved Service Request operational policies and procedures.	X	
12. Implement monthly Service Request reporting.	X	
13. Implement and maintain a service ordering process that clearly defines how to order, change or delete services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Ensure that all Service Requests are routed to the appropriate parties for timely resolution.	X	
15. Provide status, upon request of the County, of all Service Requests.	X	
16. Ensure applicable Service Requests are properly authorized and prioritized.	X	
17. Authorize closure of all Service Requests.		X
18. Manage efficient workflow of Service Request including the involvement of Third-Parties.	X	
19. Process all Service Requests.	X	
20. Update, as needed, the Service Request Management Services design for operational and technical currency.	X	
21. Produce and submit monthly reports detailing all Service Requests.	X	
22. Manage Service Request assignments throughout Service Frameworks and associated workflows as part of Service Desk responsibility.	X	
23. Make changes to the Service Request Management Services to account for all changes in the Services (e.g. new resource units, updated OIC) within 5 business days.	X	

4. END-USER SERVICES

4.1. Overview

This section pertains to the End-User Services Framework. End-User Services are composed of the following Framework Components:

- Desktop Computing Services
- Core Software Services
- County Retained Assets Services
- Mobile Device Support Services
- Unified Communications Services
- Catalog Services
- Network Printer Services
- Electronic File Synchronization and Sharing

4.2. High Level Requirements

4.2.1. Contractor shall recommend, for County approval, qualified End-User Service Manager as Contractor Key Personnel to manage End-User Services.

4.2.2. Contractor shall meet County business needs for highly available, reliable and secure End-User Services.

4.2.3. Contractor shall provide centralized management and control of all End-User Services.

4.2.4. Contractor shall improve End-User productivity and customer satisfaction in providing End-User Services.

4.2.5. Contractor shall continuously improve End-User Services and Service Levels.

4.2.6. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to operational and technical improvements of End-User Services.

4.2.7. Contractor shall develop training documentation and End-User FAQs and post them on the Service Portal.

4.2.8. Contractor shall continuously develop, use, maintain and update help desk scripts and processes for End-User Services support.

4.2.9. Contractor shall provide technology assistance and support to the County in planning and standard-setting activities.

4.2.10. Contractor shall standardize Hardware and Software across End-User Services.

4.2.11. Contractor shall improve asset tracking and reporting and shall provide updates to the Integrated Asset Management System.

4.2.12. Contractor shall support County's business initiatives by ensuring high performance with End-User Services.

4.2.13. Contractor shall provide Incident determination, Root Cause Analysis and Resolution for all End-User Services.

4.2.14. Contractor shall provide IMAR Services for the End-User Services.

4.2.15. Contractor shall maintain updated and publish End-User Services standards in the Standards and Procedures manual posted on the Service Portal.

4.3. Environment

The following further describe and scopes End-User Services elements supported by Contractor and with which Contractor shall comply.

4.3.1. Technology Refresh

Contractor shall refresh End-User Services as specified within each Framework Component, unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

4.4. Roles and Responsibilities

4.4.1. Install, Move, Add, Remove (IMAR) Services Roles and Responsibilities

IMAR Services consist of Service Requests made by End-Users for initial deployment and provisioning of Hardware, Software, office moves, etc. The Contractor shall provide IMAR activities for the End-User Services Framework. All IMAR activities require prompt updates to the Contractor's Integrated Asset Management tracking system and monitored by the Service Desk.

The following table identifies the IMAR Services roles and responsibilities that the Contractor and County shall perform.

IMAR Services Roles and Responsibilities		
General Roles and Responsibilities	**Contractor**	**County**
1. Develop and document in the Standards and Procedures Manual IMAR procedures.	X	
2. Review and approve IMAR procedures.		X
3. Conduct pre-installation and site survey activities (e.g., Network connectivity, power, data jack preparation) in accordance with the IMAR procedures and specific Service Request.	X	
4. Perform Hardware and Software IMARs and re-installations in accordance with the Service Request, IMAR procedures and other application policies (e.g., security policies).	X	
5. Conduct data and application migration that is necessary due to any Hardware or Software IMARs and re-installations.	X	
6. Update all Cross Functional management tools (e.g., Integrated Asset Management database) with required data and Close an IMAR Service Request.	X	
7. Provide basic End-User or technical staff orientation as needed when installing a new End-User Asset.	X	
8. Coordinate with Service Desk and all other necessary Third-Party and County support organizations to manage all IMAR Service Requests to resolution and closure.	X	
9. Coordinate the disposal of obsolete Assets at the direction of the County.	X	

IMAR Services Roles and Responsibilities		
10. Conduct End-User satisfaction survey after the completion of each IMAR Service Request and End-User Assets refresh.	X	
Install Roles and Responsibilities	**Contractor**	**County**
11. Order and deliver the End-User Services Asset to the End-User workspace.	X	
12. Install the End-User Services asset, including configuration, setup, and network connection.	X	
13. Perform all diagnostic testing to ensure End-User Services Framework asset functionality.	X	
14. Remove any boxes and/or packing materials.	X	
15. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	
16. Provide basic End-User or technical staff orientation when installing a new End-User Asset.	X	
Move Roles and Responsibilities	**Contractor**	**County**
17. Provide move services within a Location or from a Location to a Location, for any End-User Services Asset, which includes disconnecting, moving and reconnecting asset in accordance with the Service Request.	X	
18. Perform all diagnostic testing to ensure End-User Services asset functionality.	X	
19. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	
Add Roles and Responsibilities	**Contractor**	**County**
20. Provide upgrade or add Hardware or Software to deployed End-User Services Assets in accordance with the Service Request.	X	
21. Modify current configurations to deployed End-User Services Assets to meet approved standards.	X	
22. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	
Remove Roles and Responsibilities	**Contractor**	**County**
23. Provide Remove Services for End-User Services Assets that are being displaced due to Service Request, refresh or Incident.	X	

IMAR Services Roles and Responsibilities		
24. Promptly update Integrated Asset Management System to ensure accuracy of asset tracking.	X	

4.4.2. On-Site Technical Support Roles and Responsibilities

On-Site Technical Support consists of activities conducted on-site with End-Users to resolve Incidents, execute IMARs or other Service Requests.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with On-Site Technical Support Services.

On-Site Technical Support Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit On-Site Technical Support requirements and procedures.	X	
2. Develop and document in the Standards and Procedures Manual On-Site Technical Support procedures.	X	
3. Review and approve On-Site Technical Support requirements and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Establish and maintain appropriate equipment sparing requirements and spares inventory levels for On-Site Technical Support.	X	
5. Coordinate with the Service Desk and all other necessary Contractor, Third-Party and the County support organizations to manage all On-Site Technical Support requests to Resolution and Closure.	X	
6. Coordinate with End-User or other site staff to schedule On-Site Technical Support visit in response to an Incident or Service Request.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Dispatch appropriate Tier 2 or Tier 3 technician(s) in response to an escalated Incident or Service Request.	X	
8. Troubleshoot, diagnose and resolve Incidents for all devices, including removing and/or repairing physically broken or inoperable devices or servers.	X	

On-Site Technical Support Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
9. Conduct appropriate tests of all repaired device or server to ensure the device or server is operating appropriately.	X	
10. Obtain End-User acknowledgment for completion of Service Request.	X	

4.4.3. End-User Services Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with End-User Services.

End-User Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit Hardware and Software standards for End-User Services Assets.	X	
2. Review and approve Hardware and Software standards for End-User Services Assets.		X
3. Identify, recommend and submit End-User Services solutions that best meet County's business needs.	X	
4. Review and approve End-User Services solutions.		X
5. Perform and deliver operational planning for End-User Services capacity and performance purposes.	X	
6. Recommend and submit Hardware and Software deployment/management policies and procedures.	X	
7. Review and approve Hardware and Software deployment/management policies and procedures.		X
8. Recommend and submit Hardware and Software upgrades to End-User Services Assets.	X	
9. Review and approve Hardware and Software upgrades to End-User Services Assets.		X
10. Recommend and submit updates and patches plan to End-User Services Assets.	X	
11. Review and approve updates and patches plan to End-User Services Assets.		X
12. Update and provide to Contractor a list of high response End-Users.		X

End-User Services Roles and Responsibilities		
13. Produce and submit preventive maintenance plans consistent with OEM practices. Plans shall include equipment model and manufacturer, frequency of PM, and specific actions to be taken such as cleaning, lubricating, adjusting, inspecting, running diagnostic tests, and replacing all parts and components defined by OEM as non-User replaceable or consumable necessary to keep the equipment functioning within the OEM specifications.	X	
14. Review and approve preventive maintenance plans.		X
15. Produce and submit recommendations for "right sizing" printer to employee ratios.	X	
16. Produce and submit annual printer refresh strategy to determine the actual print need compared to the installed base.	X	
17. Produce a technology roadmap two times per contract year, for all Hardware and Software components in End-User Services Framework for current and future version including end of life for support and timelines accordingly for County review.	X	
18. Review and approve submission of Contractor provided technology roadmap for all Desktop Framework Services Hardware and Software.		X
19. Continuously update the Standards and Procedures Manual with all changes to End-User Services.	X	
Build Roles and Responsibilities	**Contractor**	**County**
20. Produce and submit all design and engineering documentation required to build, deploy and support End-User Services Assets.	X	
21. Review and approve all engineering documentation required to deploy and support End-User Services Assets.		X
22. Ensure End-User Services solutions are fully integrated with the Service Desk Services and Integrated Asset Management System processes, including, but not limited to: • A shared system and database • Direct electronic interfaces between the Service Desk agents and field service technicians • Integrated support processes involving desktop, data center, and network for remote server and telephone break-fix	X	
23. Provide all test services required to support End-User Services including providing a test laboratory that develops and verifies desktop images, as well as the support of desktop Hardware and components evaluations and demonstrations.	X	

End-User Services Roles and Responsibilities		
24. Perform desktop Software (e.g., applications, patch packages) and Hardware functionality and product compatibility testing and development in the test laboratory environment using tools and procedures that are specially designed for this purpose (test to include: unit testing, system integration testing, LAN connectivity testing, load testing, and application interconnectivity testing).	X	
25. Develop and document test scripts.	X	
26. Provide documented test results/findings of all data packets and corresponding application, entering and leaving a standard desktop build for approval prior to finalizing a desktop standard image.	X	
27. Regularly monitor Third-Party websites and other communications for new application functionality, updates, and new Software or Hardware.	X	
28. Build/Acquire updates and patches for End-User Services Assets.	X	
29. Test updates and patches for End-User Services Assets.	X	
30. Produce and submit deployment plan for updates and patches for desktop assets.	X	
31. Review and approve the deployment plan for updates and patches for desktop assets.		X
32. Produce and submit all test documentation.	X	
33. Review and approve all test documentation.		X
34. Physically connect End-User Services Assets to the network.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
35. Provide technical support to End-Users for Incident activities.	X	
36. Manage deployment efforts using formal project management tools, methodologies and standards (e.g., ITIL change and configuration management practices).	X	
37. Produce and submit to County all deployment documentation for End-User Services.	X	
38. Review and approve all deployment documentation for End-User Services.		X
39. Conduct deployment reviews and provide results to County.	X	
40. Review and approve results of deployment reviews.		X
41. Ensure that desktop technicians have the tools necessary to improve Incident resolution time and handle all Service Requests or IMARs.	X	

End-User Services Roles and Responsibilities		
42. Provide priority support for designated County High Response End-Users.	X	
43. Perform routine preventive maintenance according to the County approved preventative maintenance plans.	X	
44. Regularly review asset data and failure trends and develop plans to review and proactively repair the equipment.	X	
45. Perform predictive maintenance according to the County approved proactive repair plans.	X	
46. Provide quarterly report on Incidents based on desktop issues that includes a plan to resolve the top three issues.	X	
47. Install and configure any Hardware or Software needed to make Unified Communication and Messaging Services operational.	X	
48. Procure and own End-User Assets (e.g., Hardware, Software, operating system, personal productivity and office automation software, applicable warranty support).	X	
49. Deploy and manage End-User asset Hardware and Software	X	
50. Perform End-User Services optimization (e.g., performance, diagnostics and recovery).	X	
51. Deploy and manage Network-attached printers, storage devices and miscellaneous peripherals.	X	
52. Procure locally attached printers, storage devices and miscellaneous peripherals.	X	
53. Own locally attached printers, storage devices and miscellaneous peripherals.		X
54. Deploy and manage locally attached printers, storage devices and miscellaneous peripherals.	X	
55. Provide Tier 2 and Tier 3 support for Software as coordinated through the Service Desk.	X	
56. Provide Incident and Tier 2 support as coordinated through the Service Desk.	X	
57. Act as the interface to the Original Equipment Manufacturer (OEM) for warranty service on behalf of the County and/or act as a certified service agent and perform the service directly.	X	
58. Conduct warm transfer and/or follow-up and coordination with the OEM.	X	

4.5. Desktop Computing Services

4.5.1. Overview

This section pertains to the Desktop Computing Services Framework Component within the End-User Services Framework. The Desktop Computing Services Framework Component applies to all Hardware, Software and labor needed to maintain and support Desktop Computing Services for End-Users. Desktop Computing Services consist of activities associated with the Plan, Build and Operate of standard Hardware and Software used to support End-User Services.

4.5.2. High Level Requirements

4.5.2.1. Contractor shall provide standardization across the Desktop Computing Services Framework Component for all Hardware and Software.

4.5.2.2. Contractor shall deploy standard core software on all Desktop Computing Services Hardware.

4.5.2.3. Contractor shall recommend annually, for County approval, standards that support the End User Services.

4.5.2.4. Contractor shall ensure that each Desktop Computing Hardware recommended standard shall be available from the manufacturer for the entire Contract Year.

4.5.2.5. Contractor shall implement new Desktop Computing Hardware standards effective at the start of each Contract Year.

4.5.2.6. Contractor shall hard drive encrypt all Desktop Computing Hardware throughout the entire life-cycle.

4.5.2.7. Contractor shall ensure all Desktop Computing Hardware are installed with the defined core software standard.

4.5.2.8. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and

transformational activities related to operational and technical improvements of Desktop Computing Services.

4.5.2.9. Contractor shall provide Desktop Computing performance management consisting of measuring, modeling, planning, optimizing and reporting of Desktop Computing Services to ensure they operate with the speed, reliability and capacity to meet the needs of the County.

4.5.2.10. Contractor shall provide continuous desktop optimization to maximize response time for all County End-Users interactions with Portfolio Applications.

4.5.2.11. Contractor shall continuously maintain a timeline/roadmap of all Desktop Computing Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assist in defining the standards.

4.5.2.12. Contractor shall provide Electronic Signature Services through a reliable and secure interface to allow County users to electronically share documents with external entities for review and eSigning via web browser. Electronic documents may be signed by external entities, County staff or both.

The Electronic Signature Services shall include:

- Electronic signature and associated digital signature management
- Service Desk support
- User administration
- Electronic signature service upgrade support
- eSigner authentication support
- WORD tagging support
- Template and workflow support
- eSigned document download support
- Monthly report for e-sign transactions

4.5.2.13. Contractor shall provide the Duo Hardware Token MFA to allow County employees and partners secure access, with Multi Factor Authentication (MFA), to the County network.

4.5.3. Environment

The following sub-sections further describe and scope Desktop Computing Services elements supported by Contractor and with which Contractor shall comply.

4.5.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Desktop Computing Services.

4.5.3.2. Desktop - Standard Workstation

4.5.3.2.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.2.2. All Desktop - Standard Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.2.3. All Desktop - Standard Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.3. Desktop - Advanced Workstation

4.5.3.3.1. All Desktops - Advanced Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.3.2. All Desktops - Advanced Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.4. Desktop - Advanced Engineering Workstation

4.5.3.4.1. All Desktops - Advanced Engineering Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.4.2. All Desktops - Advanced Engineering Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.5. Desktop - Engineering Workstation

4.5.3.5.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.5.2. All Desktops - Engineering Workstations shall be refreshed within a 4-year cycle from initial installation.

4.5.3.5.3. All Desktops - Engineering Workstations shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.6. Desktop - 3D Workstation

4.5.3.6.1. All Desktop – 3D Workstations shall be refreshed within a 3-year cycle from initial installation.

4.5.3.6.2. All Desktop – 3D Workstations shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.7. Laptop - Standard

4.5.3.7.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.7.2. All Laptop - Standard assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.7.3. All Laptop - Standard assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.8. Laptop - Ultra-Portable

4.5.3.8.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.8.2. All Laptop - Ultra-Portable assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.8.3. All Laptop - Ultra-Portable assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.9. Laptop - Engineering

4.5.3.9.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.9.2. All Laptop - Engineering assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.9.3. All Laptop – Engineering assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.10. Laptop - Ruggedized

4.5.3.10.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.10.2. All Laptop - Ruggedized assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.10.3. All Laptop - Ruggedized assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.11. Laptop – Standard LTE

4.5.3.11.1. All Laptop – Standard LTE shall be refreshed within a 3-year cycle from initial installation.

4.5.3.11.2. All Laptop – Standard LTE shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.12. Tablet - Ruggedized

4.5.3.12.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.12.2. All Tablet - Ruggedized assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.12.3. All Tablet – Ruggedized assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.13. Tablet - Convertible

4.5.3.13.1. First Contract Year standards shall be those currently in effect with the Legacy Provider as of the Service Framework Transition date.

4.5.3.13.2. All Tablet - Convertible assets shall be refreshed within a 3-year cycle from initial installation.

4.5.3.13.3. All Tablet Convertible assets shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.14.Desktop Scanner

4.5.3.14.1. All Desktop Scanners shall be refreshed within a 4-year cycle from initial installation.

4.5.3.14.2. All Desktop Scanners shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.15.Desktop - Mini Workstation

4.5.3.15.1. All Desktop - Mini Workstation shall be refreshed within a 4-year cycle from initial installation.

4.5.3.15.2. All Desktop - Mini Workstation shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.16.Desktop - Engineering Workstation Gold

4.5.3.16.1. All Desktop - Engineering Workstation Gold shall be refreshed within a 4-year cycle from initial installation.

4.5.3.16.2. All Desktop - Engineering Workstation Gold shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.3.17.Tablet – Surface Pro LTE

4.5.3.17.1. All Tablet-Surface Pro LTE shall be refreshed within a 3-year cycle from initial installation.

4.5.3.17.2. All Tablet-Surface Pro LTE shall be refreshed no later than 2 months after the expiration of the 3-year cycle.

4.5.3.18.Desktop - Small Form Factor with Optical Drive

4.5.3.18.1. All Desktop - Small Form Factor with Optical Drive shall be refreshed within a 4-year cycle from initial installation.

4.5.3.18.2. All Desktop – Small Form Factor with Optical Drive shall be refreshed no later than 2 months after the expiration of the 4-year cycle.

4.5.4. Early Refresh

The County may request early refresh of Desktop Computing asset. Early refresh is determined as refresh of the Desktop Computing asset; if the asset is not within 6 months of the scheduled refresh date. County shall request early refresh via a Service Request.

4.5.5. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Desktop Computing Services.

Desktop Computing Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit all Desktop Computing Hardware and non-Hardware standards on an annual basis.	X	
2. Review and approve Desktop Computing Hardware standards.		X
3. Produce and submit yearly Desktop Computing Hardware refresh plan.	X	
4. Review and approve yearly Desktop Computing Hardware refresh plan.		X
5. Recommend and submit Desktop Computing software deployment/management policies and procedures.	X	
6. Review and approve Desktop Computing software deployment/management policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Deploy Legacy Provider desktop standards that were in effect as of the Service Framework Transition date during the first Contact Year.	X	
8. Develop core software image for Desktop Computing based on approved standards.	X	
9. Test standard core software image for Desktop Computing prior to deployment based on approved standards.	X	
10. Review results of test and approve deployment for the core software image for Desktop Computing.		X

Desktop Computing Services Roles and Responsibilities		
11. Deploy approved core software image to all Desktop Computing Assets.	X	
12. Provide staging Services for Desktop Computing at non-County Locations.	X	
13. Deploy and manage Desktop Computing Hardware and Software (e.g., operating system, personal productivity and office automation software and Services).	X	
14. Deploy software (e.g., patches, applications, drivers and operating systems) using a Contractor provided electronic software distribution tool.	X	
15. Provide a rapid response team during software deployment for assisting affected End-Users in the event a deployed package adversely affects End-Users or any systems.	X	
16. Deploy, manage, communicate and report activities related to Desktop Computing refresh.	X	
17. Review and approve reports for Desktop Computing refresh.		X
18. Develop and provide training related to the implementation of new products and services.	X	
19. Refresh all Desktop Computing Assets no later than 2 months after the expiration of a 3-year or 4-year cycle from initial installation, whichever is applicable.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
20. Provide support, including break-fix, for all Desktop Computing.	X	
21. Implement revised new desktop hardware standards so that they become effective at the start of each Contract Year.	X	
22. Encrypt hard drive of all Standard Desktops throughout the entire life cycle of the asset.	X	
23. Provide IMAR Services.	X	
24. Conduct data, End-User profile (e.g., favorites, bookmarks, MS Outlook profile) and Application migration that are necessary due to any Desktop Computing refresh, IMAR or Incident activity.	X	
25. Provide support for Desktop Computing refresh.	X	

Desktop Computing Services Roles and Responsibilities		
26. Provide core software updates, OIC software installation and new software releases for Desktop Computing Assets.	X	
27. Provide each End-User orientation on operational concepts of the new Desktop Computing at time of deployment.	X	
28. Provide and submit End-User tip sheets on such items as log on procedures, networked drives, system usage, core software, data storage and other practices that are essential to daily tasks.	X	
29. Review and approve End-User tip sheets prior to deployment.		X
30. Continually utilize automated Integrated Asset Management System tools to identify unlicensed software on desktops and servers and to pinpoint desktop devices not running the most recent antivirus software stipulated County standards and policies.	X	

4.6. Core Software Services

4.6.1. Overview

This section pertains to the Core Software Services Framework Component within the End-User Services Framework. The Core Software Services Framework Component describes the baseline, standard software installed on all Desktop Computing Assets, County Retained Assets, and other Computing Assets determined applicable by the County.

4.6.2. High Level Requirements

4.6.2.1. Contractor shall provide standardization of Core Software Services across all Desktop Computing Assets, County Retained Assets and other Computing Assets determined applicable by the County.

4.6.2.2. Contractor shall continuously maintain currency of core software standards deployed within the Desktop Computing Services Framework Component.

4.6.2.3. Contractor shall make recommendations for County approval of Core Software standards annually.

4.6.2.4. Contractor shall present and discuss Core Software standards at the County/Contractor Enterprise Architecture Governance.

4.6.2.5. Contractor shall publish Core Software standards in the Standards and Procedures Manual on the Service Portal.

4.6.2.6. Contractor shall refresh Core Software to latest standards annually for all Desktop Computing Assets and Retained Assets.

4.6.2.7. Contractor shall maintain currency, at all times, of Core Software deployed within the Desktop Computing Services and Retained Assets.

4.6.2.8. Contractor shall ensure all Desktop Computing Assets shall be deployed with the current standard Core Software.

4.6.2.9. Contractor shall ensure that there is no degradation of performance on all Core Software installed hardware.

4.6.2.10. Contractor shall ensure that optimal network performance on all Core Software installed hardware.

4.6.2.11. Contractor shall develop automated deployment strategies for Core Software installation on all hardware.

4.6.2.12. Contractor shall recommend annually, for County approval, standards that support the Core Software Services.

4.6.2.13. Contractor shall leverage all existing license agreements when recommending annual Core Software standards.

4.6.2.14. Contractor shall provide Core Software standards recommendations and submit for County approval.

4.6.2.15. Contractor shall ensure all Core Software is fully tested with all Desktop approved software to ensure the highest degree of operational integrity.

4.6.2.16. Contractor shall promptly patch and maintain all Core Software to the highest operational level throughout each Contract Year.

4.6.2.17. Contractor shall make effective new Core Software standards at the start of each Contract Year.

4.6.2.18. Contractor shall promptly update all Desktop Computing Assets to the latest Core Software standards annually or as the Core Software standards change.

4.6.2.19. Contractor shall maintain a timeline/roadmap of all Core Software Services software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Core Software that assists in defining the standards.

4.6.3. Environment

4.6.3.1. Software

Contractor shall supply all software to support Core Software Services.

4.6.4. Department of Child Support Services (DCSS) Core Software

The DCSS Core Software complies with the County Core Software standards with the following addition:

- INFO Connect version 4.1

4.6.5. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Core Software Services.

Core Software Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit annually core software standards for Desktop Computing Assets.	X	
2. Review and approve core software standards annually for Desktop Computing Assets.		X

Core Software Services Roles and Responsibilities		
3. Recommend and submit core software deployment/management policies and procedures.	X	
4. Review and approve core software deployment/management policies and procedures.		X
5. Develop a technical life cycle roadmap for each item in Core Software Services.	X	
6. Review and approve the technical life cycle roadmap for each item in Core Software Services.		X
7. Maintain all Core Software with the latest release version on all Desktop Computing Assets as defined in the approved standard.	X	
Build Roles and Responsibilities	**Contractor**	**County**
8. Maintain the same level of approved Core Software at all times for all Desktop Computing Assets.	X	
9. Develop core software image for Desktop Computing Assets based on approved standards.	X	
10. Test standard core software image for Desktop Computing Assets prior to deployment based on approved standards to ensure operational integrity.	X	
11. Review results of test and approve deployment for the core software image for Desktop Computing Assets.		X
12. Deploy approved Desktop Computing core software image.	X	
13. Engineer the core software image and provide any and all version changes, upgrades, enhancements, and additions to the core software image, to ensure that the core software image shall function properly on the desktop and the Applications Portfolio.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Provide support, including break-fix, for all Core Software Incidents.	X	
15. Provide Core Software updates, OIC software installation and new software releases for Desktop Computing Assets.	X	
16. Provide each End-User orientation on operational concepts of the new Core Software features and functions at time of deployment.	X	
17. Provide and submit End-User tip sheets on Core Software to the Service Portal.	X	

Core Software Services Roles and Responsibilities		
18. Continuously update all Core Software items including, latest patches, service releases, on all Desktop Computing Assets.	X	

4.7. County Retained Assets Services

4.7.1. Overview

This section pertains to the County Retained Assets Services Framework Component within the End-User Services Framework. County Retained Assets definition is Desktop Computing Services standard hardware purchased by the County and supported by the Contractor.

4.7.2. High Level Requirements

4.7.2.1. Contractor shall document, deliver (for County approval) and post to the Service Portal enrollment procedure for County Retained Assets.

4.7.2.2. Contractor shall document all County Retained Assets in the Integrated Asset Management System.

4.7.2.3. Contractor will maintain and support all County Retained Assets currently enrolled.

4.7.2.4. Contractor shall install standard Core Software on all County Retained Assets.

4.7.2.5. Contractor shall install the standard Core Software or DCSS Core Software for DCSS retained assets as determined by End-User Service Request.

4.7.2.6. Contractor shall exclude County Retained Assets from Desktop Computing Services refresh.

4.7.2.7. Contractor shall maintain Core Software to approved standards on County Retained Assets.

4.7.2.8. Contractor shall report to End-User the end of life of the County Retained Asset annually.

4.7.2.9. Contractor shall not exclude any County Retained Asset from the Services.

4.7.3. Environment

4.7.3.1. Hardware

The standard Desktop Computing Services Assets, published in the Standards and Procedures manual, are in scope for County Retained Assets Services.

4.7.3.2. Desktop - DCSS

4.7.3.2.1. All Desktop - DCSS owned by the State are Retained Assets.

4.7.3.2.2. All Desktop - DCSS shall follow the DCSS Core Software standards.

4.7.3.2.3. Contractor shall perform hardware refreshes for the Desktop - DCSS.

4.7.3.2.4. Desktop – DCSS will be refreshed every four years.

4.7.3.2.5. Contractor shall be responsible for IMARs, break-fix, and disposal of Desktop - DCSS in coordination with DCSS and the State.

4.7.3.3. Laptop – DCSS

4.7.3.3.1. Laptop – DCSS owned by the State shall be treated as County Retained Assets.

4.7.3.3.2. Laptop – DCSS shall follow the DCSS Core Software standards.

4.7.3.3.3. Laptop – DCSS refresh cycle shall be completed no later than 6 months after State provisioning.

4.7.3.3.4. Laptop refresh cycle shall begin upon the receipt of the initial laptop shipment from the State.

4.7.3.3.5. Contractor shall be responsible for IMARs, break-fix, and disposal for Laptop – DCSS in coordination with DCSS and the State.

4.7.3.4. Enrollment Requirements

Enrollment of County Retained Assets requirements are as follows:

- For new enrollment, the County Retained Assets must be compliant with current Desktop Computing Services hardware standards
- County Service Request is issued to initiate the enrollment process
- Contractor shall verify the requirements to enroll County Retained Assets

4.7.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with County Retained Assets Services.

County Retained Assets Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit plans for use of the Integrated Asset Management System to track Retained Assets.	X	
2. Review and approve plans for use of the Integrated Asset Management System to track Retained Assets.		X
3. Ensure that DCSS Retained Assets comply with the DCSS Core Software standards.	X	
Build Roles and Responsibilities	**Contractor**	**County**
4. Validate during enrollment, that the new Retained Assets are compliant with current Desktop Computing Services standards.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
5. Provide support, including break-fix, for all County Retained Assets Incidents.	X	
6. Provide hardware support for all County Retained Assets.	X	
7. Maintain and update the County Retained Assets inventory.	X	
8. Maintain and support County Retained Assets currently enrolled at the time of Transition.	X	
9. Tag Retained Assets with a Contractor's asset tag in addition to the existing County property tag and track these in the Integrated Asset Management System.	X	

County Retained Assets Services Roles and Responsibilities		
10. Verify Retained Asset enrollment requirements and submit to County for review and approval.	X	
11. Review and approve Retained Asset enrollment requirements.		X
12. Perform the Retained Asset enrollment.	X	
13. Install current Core Software Standard County Retained Assets.	X	
14. Install the current Core Software Standard or DCSS Core Software for DCSS Retained Assets.	X	
15. Perform hardware refresh of each DCSS Retained Assets in accordance with the State refresh standards.	X	
16. Provide IMARs, break-fix, and disposal of DCSS Retained Assets in coordination with DCSS and the State.	X	

4.8. Mobile Device Support Services

4.8.1. Overview

This section pertains to the Mobile Device Services Framework Component within the End-User Services Framework. The Mobile Device Services Framework Component applies to providing support to County End-Users in the operational and business use of County owned Mobile Devices which include Retained Assets and authorized BYOD. Mobile Device Services consist of activities associated with the Plan, Build and Operate of managed mobile devices and bring-your-own mobile devices (BYOD).

4.8.2. High Level Requirements

4.8.2.1. Contractor shall provide Service Desk Services support and End-User Services support for supported County owned Mobile Devices.

4.8.2.2. Contractor shall support End-User Mobile Devices as requested by a Service Request. Contractor shall consider this optional support.

4.8.2.3. Contractor shall enable and support connectivity for a supported Mobile Device to County resources.

4.8.2.4. Contractor shall assist End-Users with the operational use of supported Mobile Devices.

4.8.2.5. Contractor shall continuously provide, update and maintain documentation, FAQs and other related tip sheets to County End-Users via the Service Portal.

4.8.2.6. Contractor shall support End-User authentication to County resources for all supported Mobile Devices.

4.8.2.7. Contractor shall provide Incident tracking, escalation and resolution for supported Mobile Devices.

4.8.2.8. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of supported Mobile Devices.

4.8.2.9. Contractor shall continuously develop, update and maintain Service Desk scripts and processes for Mobile Device Support Services End-User support.

4.8.2.10. Contractor shall continuously update instructions, FAQs and other documentation for End-Users on the Service Portal.

4.8.2.11. Contractor shall support BYOD devices as specified in County policy.

4.8.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Mobile Device Support Services.

Mobile Device Support Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Implement mobile device support Services per the approved procedures.	X	

Mobile Device Support Services Roles and Responsibilities		
2. Produce and submit recommendations (on annual basis) the Mobile Device supportable assets standards.	X	
3. Review and approve all Mobile Device supportable assets standards recommendations.		X
4. Review and approve standardization across the managed Mobile Device Services Framework Component for all mobile hardware and software.		X
Operate Roles and Responsibilities	**Contractor**	**County**
5. Provide enterprise mobile device application store support.	X	
6. Manage County-approved BYOD devices and the installed County-approved applications on such devices.	X	
7. Deploy or remove mobile applications using the Enterprise Application Store.	X	
8. Perform device password resets as required.	X	
9. Assist End-Users with any Incidents or Incidents arising from application releases and patches.	X	
10. Coordinate Incident and Service Request resolution among End-Users, the Service Desk and Third-Parties to manage all End-User MDM related Incidents and Service Requests as needed.	X	
11. Troubleshoot and resolve access Incidents to authorized enterprise content from any authorized mobile device.	X	
12. Monitor and report the usage of self-service for mobile devices.	X	
13. Produce and submit mobile device support solutions that best meet County business needs and security policies.	X	
14. Review and approve mobile device support solutions.		X
15. Produce and submit End-User instructions on provisioning and configuration of mobile devices.	X	
16. Review and approve End-User instructions on provisioning and configuration of mobile devices.		X

Mobile Device Support Services Roles and Responsibilities		
17. Manage mobile Users enrollment and access by Active Directory (AD) group membership.	X	

4.9. Unified Communications Services

4.9.1. Overview

The Unified Communications Services Framework Component within the End-User Services Framework applies to the process allowing County End-Users to communicate efficiently and effectively through various integrated methods. Unified Communications Services provide strategy, process, methodology, support and documentation Real-Time or Non Real-Time methods deployed to End-User Services.

Real-Time methods are, but not limited to, instant messaging (IM), presence, voice, mobility, audio, desktop web & video conferencing, desktop sharing, data sharing, interactive whiteboards, call control.

Non Real-Time methods are, but not limited to, integrated voice mail, E-Mail, SMS and fax.

4.9.2. High Level Requirements

4.9.2.1. Contractor shall provide Service Desk Services support and End-User Services support for Unified Communications Services.

4.9.2.2. Contractor shall support End-User authentication to County resources for all Unified Communications Services.

4.9.2.3. Contractor shall provide, upon County approval, Unified Communications Services externally (off County network).

4.9.2.4. Contractor shall provide Incident tracking, escalation and resolution for Unified Communications Services.

4.9.2.5. Contractor shall support BYOD devices as specified in County policy for Unified Communications Services.

4.9.2.6. Contractor shall provide standardization across the Unified Communications Services client software.

4.9.2.7. Contractor shall be own, provision, maintain, update and support all Hardware and Software associated with providing Unified Communications Services.

4.9.2.8. Contractor shall deploy to all Desktop Computing Assets, Retained Assets and mobile devices client software needed to engage in Unified Communications Services.

4.9.2.9. Contractor shall maintain at all times, current standard version of Unified Communications Services client software to all Desktop Computing Assets, Retained Assets and mobile devices.

4.9.2.10. Contractor shall provide Incident tracking, escalation and resolution for Unified Communications Services.

4.9.2.11. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Unified Communications Services.

4.9.2.12. Contractor shall continuously develop, update and maintain help desk scripts and processes for Unified Communications Services End-User support.

4.9.2.13. Contractor shall recommend, for County approval, Unified Communications Services client software standards annually.

4.9.3. Environment

4.9.3.1. All Desktop Computing Services Assets shall be supported for Unified Communications Services.

4.9.3.2. All County owned and managed mobile devices shall be supported for Unified Communications Services.

4.9.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Unified Communications Services.

Unified Communications Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Unified Communications Services policies and procedures.	X	
2. Review and approve Unified Communications Services policies and procedures.		X
3. Recommend (on annual basis) the Unified Communications Services standards.	X	
4. Review and approve the recommended Unified Communications Services standards.		X
5. Develop and submit recommended standardization across the managed Unified Communications Services.	X	
6. Review and approve standardization across the managed Unified Communications Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Perform the installation, testing, and tuning of all technical environment Hardware, Software, peripherals and interfaces related to the support of Unified Communications Services platforms.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
8. Perform end-to-end Incident determination and resolution for all Unified Communications Services related Incidents.	X	
9. Provide and support Remote Access Services for Unified Communications Services for defined County resources.	X	
10. Take corrective action as needed for all Unified Communications Services.	X	
11. Coordinate Incident resolution with Technical Support, Incident & Problem Management and Third-Parties.	X	
12. Provide troubleshooting, repair and escalation of Incidents within the Unified Communications Services platform environment.	X	

Unified Communications Services Roles and Responsibilities		
13. Provide End-User training, tip sheets, FAQs and post to the Service Portal.	X	
14. Perform Incident support activities as required, remotely or on-site.	X	
15. Provide Tier 2 and 3 technical assistance and support for Unified Communications Services End-Users.	X	

4.10. Catalog Services

4.10.1. Overview

Catalog Services Framework Component of End-User Services consist of activities associated with Optional Item Catalog (OIC). The OIC contains the Hardware and Software items that are approved for the End-User Services environment; consisting of distinct categories of goods and services available for purchase by the County.

4.10.2. High Level Requirements

4.10.2.1. Contractor shall promptly publish the current OIC in the Standards and Procedures Manual as changes occur.

4.10.2.2. Contractor shall make available the updated and current OIC within the Service Request system.

4.10.2.3. Contractor shall acquire, configure, deliver, install and support OIC items throughout their useful life.

4.10.2.4. Contractor shall maintain, as changes occur, the published OIC.

4.10.2.5. Contractor shall recommend, for County approval, changes to the OIC.

4.10.2.6. Contractor shall maintain currency of all items in the OIC with recommendations to the County.

4.10.2.7. Contractor shall meet all IMAR Service Level obligations for all items in the OIC.

4.10.2.8. Contractor shall provide recommended updates, for County approval, to the OIC based on Desktop Computing Services standards.

4.10.2.9. Contractor shall provide recommend software packages that comply with Core Software standards.

4.10.2.10. Contractor shall acquire, configure, deploy, support and maintain all OIC items delivered to End-Users throughout the useful like of the OIC item.

4.10.2.11. Contractor shall configure, deploy, support and maintain, as needed, Portfolio Application client software needed for End-Users business functions.

4.10.2.12. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Catalog Services and the OIC.

4.10.2.13. Contractor shall continuously develop, update and maintain help desk scripts and processes for Catalog Services End-User support.

4.10.2.14. Contractor shall continuously maintain a timeline/roadmap of all OIC Hardware and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of Hardware and Software that assist in defining the standards.

4.10.3. Environment

The OIC categories of components are segmented and distinct categories. These categories offer organization and definition to the OIC. These segmented and distinct categories are as follows:

Desktop Peripheral Hardware	Hardware physically connected to a Desktop Computing asset, including, but not limited to, printers, scanners,

	keyboards, managed mobile devices and monitor upgrades.
Stand-Alone Hardware	Hardware that is not physically connected to a Desktop Computing asset Including, but not limited to, videoconferencing optional equipment, audio/video equipment, and replacement parts.
Desktop Software	Classified in accordance with the Desktop Applications Directory (DAD). Includes acquisition, license management, engineering, deployment, rights management, and full maintenance of the software by the Contractor. The County shall manage the DAD, including adds, deletes, and updates of approved Applications on the list.
Portfolio Application Client Software	Portfolio Application client software not otherwise covered by a Resource Unit (i.e., Non-DAD Commercial Off-the-Shelf ("COTS") Software).
IT Training Courses	IT Training Courses as needed to support County business needs and enterprise license agreements.

4.10.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Catalog Services:

Catalog Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define, add, modify and delete Hardware and Software items in Optional Item Catalog (OIC).		X
2. Produce and submit recommendations for updates to Hardware and Software items in the OIC.	X	
3. Review and approve updates to Hardware and Software items in the OIC.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Maintain currency of items in the OIC.	X	

Catalog Services Roles and Responsibilities		
5. Host and make available the OIC to County Users on a proven table-driven catalog management system.	X	
6. Organize the OIC to facilitate ordering and viewing for End-Users.	X	
7. Publish the OIC on the Service Portal, with online help functions, for viewing and ordering.	X	
8. Provide all engineering necessary to ensure functionality of all Hardware and Software items in the OIC with Desktop Computing Assets.	X	
9. Test all new and updated Hardware and Software items listed in the OIC prior to deployment.	X	
10. Develop and submit a deployment plan for any multi-End-User OIC implementations.	X	
11. Review and approve deployment plan for any multi-End-User OIC implementations.		X
12. Publish all new and updated items in the OIC at the conclusion of the engineering activity.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
13. Authorize items to be included in OIC.		X
14. Add or modify the DAD listed in the OIC via a Service Request.	X	
15. Maintain and support (as listed in the "Level of Support" section of the OIC), including break-fix, all Software and Hardware in the OIC.	X	
16. Provide IMAR Services for OIC items.	X	
17. Maintain and publish on a monthly basis the OIC.	X	
18. Provide Web access and ordering abilities for the OIC to all County End-Users.	X	
19. Provide ongoing OIC User training.	X	
20. Provide End-User orientation on operational concepts of new Hardware or Software installed via order from the OIC.	X	
21. Review new manufacturers' product posted offerings, verify the currency of the listed equipment, and maintain the accuracy of the OIC.	X	

4.11. Network Printer Services

4.11.1. Overview

This section pertains to the Network Printer Services Framework Component within the End-User Services Framework. The Network Printer Services Framework Component applies to all Hardware, Software and back-end infrastructure needed to maintain and support networked Printer Assets. Network Printer Services consist of the activities associated with the Plan, Build and Operate of all networked Printer Assets.

4.11.2. High Level Requirements

4.11.2.1. Contractor shall provide recommend standards, for County approval, annually for Network Printer Services.

4.11.2.2. Contractor shall provide a redundant, highly available, and technical current back-end infrastructure to support Network Printer Services.

4.11.2.3. Contractor shall deploy and manage back-end infrastructure that is redundant with complete fail-over minimizing any associated print service Incident.

4.11.2.4. Contractor shall maintain currency on all print drivers used to deliver the Network Printer Services.

4.11.2.5. Contractor shall maintain currency, at all times, of Network Printer Assets firmware.

4.11.2.6. Contractor shall determine, with County approval, categories of Network Printer Assets.

4.11.2.7. Contractor shall ensure that each Network Printer recommended standard be available from the manufacturer for the entire Contract Year.

4.11.2.8. Contractor shall publish in the OIC the standards for Network Printer Services.

4.11.2.9. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Network Printer Services.

4.11.2.10. Contractor shall continuously develop, update and maintain help desk scripts and processes for Network Printer Services End-User support.

4.11.2.11. Contractor shall leverage existing license agreements to the extent possible for all Network Printer Services.

4.11.2.12. Contractor shall make effective new Network Printer standards at the start of each Contract Year.

4.11.2.13. Contractor shall supply, via Service Portal, a list of consumables, updated annually or as standards change, for current printers deployed to County End-Users in the environment.

4.11.2.14. Contractor shall exclude Printers not attached or connected to the County network.

4.11.2.15. County shall be responsible for Network Printer consumables which are defined as paper and ink/toner.

4.11.2.16. Contractor shall be responsible for all maintenance and availability, including break-fix, of Network Printer Services.

4.11.2.17. Contractor shall maintain and update annually a timeline/roadmap of all Core Software versions and life cycles to adequately plan timeframes and completion dates to stay within supported versions.

4.11.3. Environment

4.11.3.1. Hardware

The County current Network Printer standards fall into the following categories:

- Monochrome Network Workgroup Printer — Standard Format (abbreviated as "MNWP")
- Monochrome Network Workgroup Printer — Large Format (11x17) (abbreviated as "MNWP-LF")
- Monochrome Network High Volume Printer — Large Format (11x17) (abbreviated as "MNWP-LF-H")
- Color Network Workgroup Printer — Large Format (abbreviated as "CNWP-LF")
- Color Network Workgroup Printer — Standard Format (abbreviated as "CNWP")

4.11.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Network Printer Services.

Network Printer Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Recommend and submit Network Printer Assets policies, procedures and Hardware standards on an annual basis.	X	
2. Review and approve Network Printer Assets policies, procedures and hardware standards.		X
3. Produce and submit the annual Network Printer asset refresh plan.	X	
4. Review and approve the annual Network Printer asset refresh plan.		X
5. Provide standardization across the Network Printer Services Framework Component for all Hardware and Software.	X	
Build Roles and Responsibilities	**Contractor**	**County**
6. Determine which multifunction or specialized printer devices shall be purchased.	X	
7. Review and approve the purchase of the multifunction or specialized printer devices.		X
8. Provide network connectivity and print queue installation for County purchased. Such devices shall be reviewed with Contractor prior to selection.	X	

Network Printer Services Roles and Responsibilities		
9. Provide staging Services for Network Printer Assets at non-County locations.	X	
10. Deploy and manage Network Printer Hardware and Software (e.g., printer drivers).	X	
11. Deploy, manage, communicate and report activities related to Network Printer refresh.	X	
12. Review and approve reports for Network Printer refresh.		X
13. Identify the IT Coordinator for each deployed Network Printer prior to transition or deployment.	X	
14. Develop and provide training related to the implementation, use and operation of Network Printers.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
15. Perform the Network Printer hardware asset refresh not later than two months after the expiration of the four-year cycle.	X	
16. Provide support, including break-fix, for all Network Printer Assets.	X	
17. Provide Network Printer IMAR Services.	X	
18. Provide support for Network Printer Assets refresh.	X	
19. Provide printer driver updates.	X	
20. Provide each departmental IT coordinator orientation on operational concepts of the new printer asset at time of deployment.	X	
21. Order and replace toner cartridges and paper from County office supply sources.	X	

4.12. Electronic File Sharing and Synchronization Services

4.12.1. Overview

This section pertains to the Electronic File Sharing Services (EFSS) component within the End User Services Framework. The Electronic File Sharing Services Framework Component applies to all Hardware, Software and labor needed to maintain and support EFFS.

4.12.2. High Level Requirements

4.12.2.1. Contractor shall provide, maintain and support a centralized, secure EFSS with access through browsers on approved and managed County computing devices.

4.12.2.2. Contractor shall provide EFSS with granular permissions to protect confidential, sensitive and public information that may be posted.

4.12.2.3. Contractor shall provide EFSS that allows County users to share and collaborate on files internally and externally.

4.12.2.4. Contractor shall provide EFSS that allows external users to consume or share files to and/or from County users.

4.12.2.5. Contractor shall provide standard County single sign-on for authenticating County Active Directory users.

4.12.2.6. Contractor shall provision County users to access EFSS as per authorized Service Request.

4.12.2.7. Contractor shall provide County users with the ability to create temporary secure locations for sharing files that are too large for email. The temporary secure location shall be accessible to County users and external users with access expiring after designated time period as set by sharing party or after twenty-four (24) hours, whichever is less.

4.12.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with EFFS.

Electronic File Sharing Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Implement EFFS as per approved procedures.	X	
2. Produce and submit plans for updates/upgrades to EFSS.	X	

Electronic File Sharing Services Roles and Responsibilities		
3. Review and approve plans for updates/upgrades to EFSS.		X
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide onboarding support for EFSS.	X	
5. Provide, update and maintain documentation, FAQs and other related tip sheets to County End Users via the Service Portal.	X	
6. Assist End Users with any Incidents associated with EFSS.	X	
7. Maintain and support EFSS. This includes maintaining all the integration points (e.g., Single Sign On, Content Delivery Network services), break-fix, etc.	X	
8. Provide IMAR Services for EFSS.	X	
9. Provide operational reports for EFSS.	X	

4.13. Audio/Video (A/V) Conference Rooms Services

4.13.1. Overview

This section pertains to the A/V Conference Rooms Installation Services Framework Component within the End User Services Framework. The A/V Conference Rooms Services Framework Component applies to the installation and support for Audio/Video Conference Rooms.

4.13.2. High Level Requirements

4.13.2.1. Contractor shall provide three (3) standardized Audio/Video Conference Rooms Services:

a. A/V Conference Room - Small
b. A/V Conference Room - Medium
c. A/V Conference Room - Large

4.13.2.2. Audio/Video Conference Rooms Services shall include the following:

- Equipment
- Equipment installation
- 3-year System support

The above items are defined in Exhibit 4.3-2 Audio/Video Conference Rooms Configuration and Support.

4.13.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Audio/Video Conference Rooms Services.

Audio/Video Conference Rooms Installation Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Submit request to initiate Audio/Video Conference Rooms installation indicating Conference Room size.		X
2. Produce and submit plans for Audio/Video Conference Rooms installation.	X	
3. Review and approve plans for Audio/Video Conference Rooms installation.		X
4. Produce and submit procedures for Audio/Video Conference Rooms installation.	X	
5. Review and approve procedures for Audio/Video Conference Rooms installation.		X
Build Roles and Responsibilities	**Contractor**	**County**
6. Design and implement Audio/Video Conference Rooms installation.	X	
7. Approve design and implementation of Audio/Video Conference Rooms installation.		X
Operate Roles and Responsibilities	**Contractor**	**County**
8. Support Audio/Video Conference Rooms as defined in Exhibit 4.3-2 Audio/Video Conference Rooms Configuration and Support.	X	

4.14. Digital Signage Services

4.14.1. Overview

This section pertains to the Digital Signage Services Framework Component within the End User Services Framework.

Services provided by this Framework Component include, but are not limited to, the following:

- Automatically download text, images and other content from websites
- Extract data in multiple formats
- Connect and Control screens over the internet
- Send extracted data to specified location

4.14.2. High Level Requirements

4.14.2.1. Contractor shall procure Digital Signage subscription services and/or devices.

4.14.2.2. Contractor shall renew Digital Signage subscriptions services with County approval.

4.14.2.3. Contractor shall provide installation, incident support, escalation, and resolution for Digital Signage Services.

4.14.2.4. Contractor shall replace a defective Digital Signage device within the warranty period.

4.14.2.5. Contractor will provide for purchase, via the OIC, Digital Signage services and/or devices.

4.14.3. Environment

The following further describe, and scope Digital Signage Services elements supported by Contractor and with which Contractor shall comply.

4.14.3.1. Hardware and Software

Contractor shall provide all devices, needed to provide the Digital Signage Services as offered by Third Party.

4.14.3.2. Technology Upgrade and Refresh

Digital Signage devices supported within the Digital Signage Services are eligible for refresh or upgrade on a three-year subscription cycle and provided for purchase, via the OIC.

4.14.4. Roles and Responsibilities

Digital Signage Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Provide Digital Signage Services recommendations and specifications.	X	
2. Review and approve Digital Signage Services recommendations and specifications.		X
3. Develop IMAR and Incident process flows for Digital Signage Services.	X	
4. Develop OIC plans for approved Digital Signage Services.	X	
5. Provide OIC information for Digital Signage Services.	X	
6. Review and approve plans for Digital Signage Services processes.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Implement Digital Signage Services inventory process.	X	
8. Implement Digital Signage Services device warranty management.	X	
9. Implement Help Desk scripts for Digital Signage Services issues.	X	
10. Deploy OIC offerings for Digital Signage Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
11. Provision Digital Signage Services as ordered by the County.	X	
12. Provide IMAR and Incident services for Digital Signage Services.	X	
13. Manage Asset Management database of Digital Signage Services for warranty and upgrade/refresh purposes.	X	
14. Provide in-warranty Digital Signage Services devices replacement as needed.	X	
15. Provide for on-site Digital Signage Services for incidents.	X	

4.15. Reserved.

4.16. Survey Solution Support Services

4.16.1. Overview

This section pertains to the Survey Solution Support Services component within the End User Services Framework. Survey Solution is designed to collect, assess, and share survey responses.

4.16.2. High Level Requirements

4.16.2.1. Contractor shall migrate existing County users based upon County-approved plan.

4.16.2.2. Contractor shall migrate existing survey data based upon County-approved plan.

4.16.2.3. Contractor shall provide Service Desk support services, including for external users.

4.16.2.4. Contractor shall be responsible for managing Administrative Users per authorized Service Requests. Administrative Users control the workgroups, create subdivisions of such workgroups, invite County Casual Users, and control the sharing of data across workgroups. Administrative Users must have an sdcounty.ca.gov email address.

4.16.2.5. Contractor shall allow for an unlimited number of Casual Users. Casual Users have view/collaboration privileges only as subordinate to one or more Administrative Users and can send surveys with less than 10 questions.

4.16.2.6. Contractor shall be responsible for managing top-level workgroups per authorized Service Requests.

4.16.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Survey Solution Support Services.

Survey Solution Support Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop plan for County review for implementation, operations, and support, including (but not limited to) asset management, incident management, Service Portal updates, annual procurement support, user and data migration activities, workgroup definitions and activities, documentation, required integration points, required reporting, etc.	X	
2. Review implementation, operations, and support, including (but not limited to) asset management, incident management, Service Portal updates, annual procurement support, user and data migration activities, workgroup definitions and activities, documentation, required integration points, required reporting, etc.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Responsibility to execute the Implementation portion of the Plan developed in the Plan R&R.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Responsibility to execute the Support portion of the Plan developed in the Plan R&R.	X	

5. NETWORK SERVICES

5.1. Overview

Network Services Framework includes the Hardware, Software and services associated with the transport of voice, video and/or data across the infrastructure, internet, data centers, and cloud based services and/or external Third-Parties to/from End-Users. Activities included are the plan, build, and operate of networked assets and services used for the transport of voice, video and/or data.

Network Services Framework includes the following Framework Components:

- Data Network Services
- Remote Access Services
- Voice Services
- Network Security Services
- Video Conferencing Services
- Video Streaming and Archiving Services
- Mobility Infrastructure Services
- Wireless Network Access Services
- Third-Party Network Access Services
- External DNS Management Services
- IP Address Management Services
- New Site Installation Services

5.2. High Level Requirements

5.2.1. Contractor shall recommend, for County approval, qualified Network Service Manager as Contractor Key Personnel to manage Network Services.

5.2.2. Contractor shall provide a reliable, scalable, responsive and secure data network with connectivity to all Locations.

5.2.3. Contractor shall provide highly available, scalable, reliable, and secure voice services with features and functions that meet or exceed County business requirements.

5.2.4. Contractor shall continuously improve Network Services.

5.2.5. Contractor shall provide all Network Services across, at a minimum, two Point of Presence locations within the County that maintains complete failover and redundancies for all Network Services.

5.2.6. Contractor shall implement a dedicated, secure, high capacity, and redundant backbone with County defined bandwidth that shall be dual homed across the two Point of Presence Locations.

5.2.7. Contractor shall provide redundant, secure, diverse Internet connections for County End-Users at each Point of Presence location.

5.2.8. Contractor shall ensure County business continues to operate during any unplanned event or outage.

5.2.9. Contractor shall provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Network Services.

5.2.10. Contractor shall continuously investigate emerging technology and services that improve the overall network efficiencies, lowers overall network costs and improves End-User network performance and security.

5.2.11. Contractor shall provide technology assistance and support to the County in planning and standardsetting activities.

5.2.12. Contractor shall maintain a secure network perimeter.

5.2.13. Contractor shall provide secure network remote access to County End-Users and authorized Third-Parties.

5.2.14. Contractor shall provide bandwidth, as County deems necessary, to accommodate the County needs and for the Services.

5.2.15. Contractor shall measure and report bandwidth consumption across all Network Services.

5.2.16. Contractor shall incorporate technology security improvements for business requirements without compromising the security, integrity, and performance of the County enterprise and information resources.

5.2.17. Contractor shall refresh and consolidate network assets to ensure operability, supportability and performance.

5.2.18. Contractor shall continuously identify and correct, with County approval, any single point failures found within Network Services.

5.2.19. Contractor shall perform centralized management and performance monitoring of Network Services.

5.2.20. Contractor shall provide network bandwidth as needed to meet County performance and operational requirements.

5.2.21. Contractor shall ensure that all Sites have sufficient bandwidth, at all times, to support the Services.

5.2.22. Contractor shall ensure that all Network Services Hardware and Software are operating at optimal and maximum performance.

5.2.23. Contractor shall report performance and capacity results monthly on Network Services.

5.2.24. Contractor shall ensure that all Network Services Hardware and Software related to network security are physically located in secure Locations.

5.2.25. Contractor shall interconnect all Sites to facilitate endtoend business functions and allow network access to shared resources.

5.2.26. Contractor shall maintain a timeline/roadmap of all Network Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

5.2.27. Contractor shall configure, install, activate, monitor and provide break-fix support to County for equipment and circuits funded through the E-Rate Program, as agreed to and defined in the Standards and Procedures (SnP) Manual for the San Diego County Branch Libraries.

5.3. Environment

5.3.1. Scope of Environment

Network Services shall cover all County Locations.

5.3.2. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Network Services.

5.3.3. Facilities

5.3.3.1. County

Network Services for all County Locations.

5.3.3.2. Contractor

Network Services for Contractor Locations used by the Contractor to provide the Services.

5.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Network Services.

Network Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Collaborate with Third-Party network carriers and other industry leaders on an initial and ongoing basis to develop and establish the most favorable, cost-effective strategic direction for voice technology for the County.	X	
2. Produce and submit network architecture documentation.	X	
3. Review and approve network architecture documentation.		X
4. Produce and submit network asset refresh plan.	X	
5. Review and approve network asset refresh plan.		X
6. Produce and submit capacity and trending analysis for network infrastructure.	X	
7. Review and approve capacity and trending analysis for network infrastructure.		X
8. Produce and submit impact analyses and associated plans.	X	
9. Review and approve impact analyses and associated plans.		X

Network Services: Plan, Build and Operate Roles and Responsibilities		
10. Produce and submit standards for network cable plant to include wiring standards, fiber standards, terminations, faceplates, cable run, and cable type.	X	
11. Review and approve standards for network cable plant to include wiring standards, fiber standards, terminations, faceplates, cable run, and cable type.		X
12. Produce and submit recommendations on maintaining the network cable plant to industry standard.	X	
13. Review and approve recommendation on maintaining the network cable plant to industry standard.		X
14. Produce and submit plans for Site additions or deletions upon request.	X	
15. Review and approve plans for Site additions or deletions upon request.		X
16. Recommend network capacity thresholds.	X	
17. Approve network capacity planning thresholds.		X
18. Provide consulting for strategy and direction including architecture consultative support.	X	
Build Roles and Responsibilities	**Contractor**	**County**
19. Design and implement network architecture based on approved documentation.	X	
20. Design, configure, deploy and report network assets based on the approved refresh plan.	X	
21. Review and approve network asset refresh plan.		X
22. Design and implement changes to the network infrastructure based on results of the capacity and trending analysis.	X	
23. Design and implement changes to the network infrastructure based on impact analyses and associated plans.	X	
24. Design and implement approved recommendations on maintaining the network cable plant to industry standard.	X	
25. Implement network cable plant standards.	X	

Network Services: Plan, Build and Operate Roles and Responsibilities		
26. Design and implement network devices to meet County availability requirements (e.g., ensure that critical servers such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Active Directory, E-Mail, etc. have dual-attached network interface cards (NICs) to independent LAN switches and/or have backup servers).	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Provide maintenance and support for all Network Services, including the cable plant, network hardware and circuits.	X	
28. Perform proactive 24/7/365 network monitoring and maintenance functions for all Framework Components (e.g., voice systems, video systems, and data network transport) from County-approved network operations centers (NOC).	X	
29. Manage all network devices in accordance with County's policies (including security oversight and change management policies).	X	
30. Manage User accounts as needed for access and maintaining network resources (e.g., logon User-id and password maintenance).	X	
31. Maintain and provide verified information including access, general logs, application logs in accordance with County's security policies.	X	
32. Ensure that network administration activities are coordinated through defined change management processes.	X	
33. Support and manage network cable plant to approved standards.	X	
34. Provide updates to network Standards documentation as required.	X	
35. Synchronize all network device time clocks using appropriate tools that meets county requirements (e.g., Network Time Protocol (NTP)).	X	
36. Backup network device configurations.	X	
37. Review and approve Services and standards for all network Services.		X
38. Respond and resolve data network-related Incidents.	X	
39. Provide management of hardware refresh activities for network infrastructure.	X	

Network Services: Plan, Build and Operate Roles and Responsibilities		
40. Manage and perform refresh of Network hardware per County standard hardware refresh cycles.	X	

5.5. Data Network Services

5.5.1. Overview

This section pertains to the Data Network Services Framework Component within the Network Services Framework. The Data Network is the transport layer of a converged network with voice, video and data communications coexisting seamlessly.

Services provided within this Framework Component include, but are not limited to, the following:

- Network management
- Network capacity and performance monitoring
- Site to site connectivity
- Bandwidth management
- End-User to network connectivity
- Network engineering
- Internet access
- Hardware and Software refresh
- Technology transformation to improve overall service delivery
- Uninterrupted Power Supply (UPS) equipment support

5.5.2. High Level Requirements

5.5.2.1. Contractor shall maintain currency on Data Network Services Hardware and Software.

5.5.2.2. Contractor shall maintain an accurate and up-to-date inventory of all Data Network Services Hardware and Software.

5.5.2.3. Contractor shall standardize, with County approval, all Hardware and Software used in the delivery of Data Network Services.

5.5.2.4. Contractor shall provide bandwidth, as needed, for all Data Network Services, including the Internet, in support of the Services.

5.5.2.5. Contractor shall provide continuous monitoring and corrective action of the Data Network Services, 24/7/365.

5.5.2.6. Contractor shall participate in continuous architecture planning of upgrades, refresh and transformational activities related to operational and technical improvements of Data Network Services.

5.5.2.7. Contractor shall design all Wide-Area-Networks (WAN) with requirements for cloud connectivity.

5.5.2.8. Contractor shall continuously assess network impact of County adoption of cloud based services.

5.5.2.9. Contractor shall participate in County cloud review committee.

5.5.2.10. Contractor shall centralize the management of Data Network Services including cloud activity.

5.5.2.11. Contactor shall include cloud services in Service Levels.

5.5.2.12. Contractor shall provide network performance management consisting of measuring, modeling, planning, optimizing and reporting of Data Network Services to ensure they carry traffic with the speed, reliability and capacity to meet the needs of the County.

5.5.2.13. Contractor shall manage network performance by continuously measuring delay, packet loss, retransmissions, and throughout.

5.5.2.14. Contractor shall promptly correct and reported performance or capacity Incidents with Data Network Services.

5.5.2.15. Contractor shall perform monitoring and break/fix support and break/fix support of Contractor provided UPS equipment.

5.5.2.16. Contractor shall perform active and passive techniques for measuring and analyzing network performance as needed to support Incident Management and Problem Management.

5.5.3. Environment

The following further describe and scope Data Network Services elements supported by the Contractor and with which Contractor shall comply.

5.5.3.1. Technology Refresh

Contractor shall refresh Data Network Services core hardware and software on a 4-year refresh schedule and Data Network Services LAN Switch hardware and software on a 5-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.5.3.2. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of services for Data Network Services.

5.5.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Data Network Services.

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendation for Data Network Services architecture.	X	
2. Review and approve recommendations for Data Network Services architecture.		X
3. Produce and submit Data Network Services refresh plan on a yearly basis.	X	
4. Review and approve Data Network Services refresh plan on a yearly basis.		X
5. Identify, recommend and submit Data Network Services solutions that best meet County business needs.	X	

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
6. Review and approve Data Network Services.		X
7. Perform and submit recommendations for Data Network Services capacity and performance policies and procedures.	X	
8. Review and approve recommendations for Data Network Services capacity and performance policies and procedures.		X
9. Produce and submit recommendations for Data Network Services migration to current technology.	X	
10. Review and approve recommendations for Data Network Services migration to current technology.		X
11. Produce and submit operational policies and procedures for monitoring and maintaining Data Network Services.	X	
12. Review and approve operational policies and procedures for monitoring and maintaining Data Network Services.		X
13. Produce and submit network provisioning policies and procedures.	X	
14. Review and approve network provisioning policies and procedures.		X
15. Produce and submit network administration policies and procedures.	X	
16. Review and approve network administration policies and procedures.		X
17. Produce and submit documentation of Data Network Services asset configuration files and IP addressing schemas.	X	
18. Review and approve documentation of Data Network Services asset configuration files and IP addressing schemas.		X
Build Roles and Responsibilities	**Contractor**	**County**
19. Produce and submit to County all design and engineering documentation to support Data Network Services.	X	
20. Review and approve all design and engineering documentation for Data Network Services.		X
21. Design, test and implement approved Data Network Services architecture.	X	
22. Deploy, manage, communicate and report on activities related to Data Network Services refresh.	X	

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
23. Review and approve Data Network refresh report.		X
24. Design and Implement Data Network Services capacity and performance policies and procedures.	X	
25. Design, test and implement Data Network Services migration to current technology.	X	
26. Implement operational policies and procedures for monitoring and maintaining Data Network Services.	X	
27. Design and implement network provisioning policies and procedures.	X	
28. Implement approved recommendations for Sites additions or deletions.	X	
29. Implement approved network administration policies and procedures.	X	
30. Order and expedite WAN circuits, Assets and Services.	X	
31. Configure Data Network Assets prior to installation.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
32. Provide support, including break-fix, for all Data Network Services.	X	
33. Manage public carriers and other circuit Third-Parties to ensure delivery of WAN Services.	X	
34. Monitor Data Network Services to established baseline and thresholds.	X	
35. Provide and support Data Network Services refresh.	X	
36. Provide and support Data Network Services migration to new technology or architecture.	X	
37. Produce and submit Data Network Services utilization, capacity and performance reports monthly.	X	
38. Review and approve requirements for WAN/LAN/VPN/Firewall Services.		X
39. Provide LAN/WAN connectivity to Locations.	X	
40. Manage and support provisioning of new and upgraded Data Network Services.	X	

Data Network Services: Plan, Build and Operate Roles and Responsibilities		
41. Procure, provision and maintain all network components and circuits.	X	
42. Provide support in accordance with approved network administration policies and procedures.	X	
43. Perform day-to-day network operations and administration activities.	X	
44. Maintain TCP/IP addressing schemes, router configurations, routing tables, VPN configurations, network addresses, MAC addresses, etc.	X	
45. Support legacy data networks and associated terminals, controllers and CSU/DSU, tied to current mainframe and midrange platforms.	X	
46. Manage LAN infrastructure, including wiring, patch panels, jack configuration and documentation.	X	
47. Implement measures for proactive monitoring and self-healing to limit network Incidents.	X	
48. Identify network Incidents and resolve in accordance with Incident Management Services.	X	
49. Perform and support physical (e.g., equipment) and logical (e.g., IP address change) IMAR associated with Sites for LAN/WAN and transport environments.	X	
50. Manage the performance of public carriers (and other Third-Parties) to meet defined schedules, Project plans, and performance.	X	
51. Coordinate ordering, procurement and inventory management of network circuits from public carriers.	X	
52. Perform point-to-point and promiscuous network traffic analysis.	X	
53. Provide monitoring and break/fix support for Contractor supplied UPS equipment.	X	

5.6. Remote Access Services

5.6.1. Overview

This section pertains to the Remote Access Services Framework Component within the Network Services Framework. Services provided by this Framework Component include,

but are not limited to, the provision of a persistent, secure, and wireless connection to internal County-networked Hardware, Software and applications from outside the County network perimeters for authorized End-Users on a 24/7/365 basis.

Services provided within this Framework Component include, but are not limited to, the following:

- VPN
- Mobile VPN
- Akamai Enterprise Application Access (EAA)
- Network persistence
- Application persistence
- Network access control
- Application tunneling
- External and mobile authentication
- Active directory account integration
- Integration with the County certificate authority
- Technology refresh

5.6.2. High Level Requirements

5.6.2.1. Contractor shall maintain a safe, reliable and secure session that allows County End-Users and authorized external Users access to designated County network resources.

5.6.2.2. Contractor shall continuously identify and correct, with County approval, any single point failures with Remote Access Services.

5.6.2.3. Contractor shall provide network persistence as part of the Remote Access Services and shall be referred to as Virtual Private Network Level 1.

5.6.2.4. Contractor shall provide application persistence as part of the Remote Access Services and shall be referred to as Virtual Private Network Level 2.

5.6.2.5. Contractor shall provide network access control (NAC) to all Remote Access Services.

5.6.2.6. Contractor shall apply County approved security policies to all Remote Access Services.

5.6.2.7. Contractor shall provide End-User Authentication for all Remote Access Services.

5.6.2.8. Contractor shall provide secure application tunneling or similar HTTP/SSL tunneling technology for County End-Users.

5.6.2.9. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Remote Access Services.

5.6.2.10. Contractor shall develop training documentation and End-User FAQs and post it on the Service Portal for County End-Users.

5.6.2.11. Contractor shall develop, use, maintain and update help desk scripts and processes for Remote Access Services End-User support.

5.6.2.12. Contractor shall provide secure, external facing portal access to County applications for approved End-Users.

5.6.3. Environment

The following further describe and scope Remote Access Services elements supported by Contractor and with which Contractor shall comply.

5.6.3.1. Technology Refresh

Contractor shall refresh Remote Access Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.6.3.2. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools and Akamai Enterprise Application Access cloud services needed in the delivery of Remote Access Services.

5.6.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Remote Access Services.

Remote Access Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for a consolidated Remote Access Services architecture.	X	
2. Review and approve recommendations for Remote Access Services architecture.		X
3. Produce and submit operational policies and procedures for Remote Access Services.	X	
4. Review and approve operational policies and procedures for Remote Access Services.		X
5. Produce and submit plans for updates and patches to Remote Access Services.	X	
6. Review and approve plans for updates and patches to Remote Access Services Assets.		X
7. Produce and submit Remote Access Services reporting requirements.	X	
8. Review and approve Remote Access Services reporting requirements.		X
9. Recommend Remote Access Services Desktop Application.	X	
Build Requirements, Roles and Responsibilities	**Contractor**	**County**
10. Design, test and implement County-approved Remote Access Services.	X	
11. Design and implement County-approved operational policies and procedures for Remote Access Services.	X	
12. Design, test and implement approved plans for updates and patches to Remote Access Services.	X	
Operate Requirements, Roles and Responsibilities	**Contractor**	**County**

Remote Access Services: Plan, Build and Operate Roles and Responsibilities		
13. Provide support, including break-fix, for all Remote Access Services Assets.	X	
14. Maintain, support and report on Remote Access Services.	X	
15. Review and approve report on Remote Access Services.		X
16. Maintain and support County Locations requiring Remote Access Services.	X	
17. Maintain and support approved operational policies and procedures.	X	

5.7. Voice Services

5.7.1. Overview

This section pertains to the Voice Services Framework Component within the Network Services Framework. The Voice Services Framework Component applies to Hardware and Software needed to operate the telecommunications systems within the County.

Services provided within this Framework Component include, but are not limited to, the following:

- Single and multi-line voice services
- Single and multi-line Voice over Internet Protocol (VoIP) services
- Voice Mail
- Local dial plans
- Long distance plans
- Voice mail to E-Mail
- Basic and Simple Interactive Voice Services
    - Basic and Simple Interactive Voice Service are defined as the support for Auto Attendant and Automated Call Distributor services as a right to use feature within Voice Services. Functionality is inherent to the Avaya enterprise voice network.
- Auto Attendants
- Automated Call Distribution (ACD)
- Analog jacks
- Short Messages Services

- Telephone handsets
- IP Conference Phones
- 4-1-1 operator Services
- Virtual Phone

5.7.2. High Level Requirements

5.7.2.1. Contractor shall interconnect all Locations along a common voice network to facilitate end-to-end business functions, reduce toll calls and lower costs.

5.7.2.2. Contractor shall provide Voice Services as a highly converged and highly redundant part of Network Services.

5.7.2.3. Contractor shall utilize SIP trunking internally and externally to provide cost optimization and network efficiency for Voice Services.

5.7.2.4. Contractor shall continuously maintain technical currency and modernization of Voice Services.

5.7.2.5. Contractor shall deploy VOIP services to all new County Sites.

5.7.2.6. Contractor shall, on Service Request, upgrade County Site to VOIP services.

5.7.2.7. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Voice Services.

5.7.2.8. Contractor shall provide Voice Mail Services that can be transcribed and delivered to County End-User E-Mail as requested by the County.

5.7.2.9. Contractor shall continuously identify and correct, with County approval, any single point failures with Voice Services.

5.7.2.10. Contractor shall develop plan, implement and integrate Unified Communication Services into Voice Services.

5.7.2.11. Contractor shall develop plan, implement and integrate Voice Services onto Desktop Computing Services Assets.

5.7.2.12. Contractor shall implement, maintain and support basic and simple IVS systems.

5.7.2.13. Contractor shall recommend a plan for County approval, and execute the approved plan for changes to continuously reduce County usage costs for Voice Services.

5.7.2.14. Contractor shall deploy and maintain VoIP Services to appropriate quality of service.

5.7.2.15. Contractor shall enable a Switched Ethernet connection (Power over Ethernet (POE)) for VoIP Services.

5.7.2.16. Contractor shall continuously provide and update documentation that details operation and use VoIP services and post them on the Service Portal Users.

5.7.2.17. Contractor shall recommend, for County approval, technology and architectural standards on a yearly basis for all Voice Services.

5.7.3. Environment

The following further describe and scope Voice Services elements supported by Contractor and with which Contractor shall comply.

5.7.3.1. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Voice Services.

5.7.3.2. Technology Refresh

Contractor shall refresh Voice Services Hardware and Software on a 5-year refresh schedule unless otherwise agreed by the County in writing, and at a

County-approved deployment schedule that minimizes disruption and reduces risk.

5.7.3.3. Single-Line Voice Services

Single-Line Voice Services are all the Hardware, Software and services necessary to provide single-line phone services to End-Users.

5.7.3.4. Multi-Line Voice Services

Multi-Line Voice Services are all the Hardware, Software and services necessary to provide multi-line phone services to End-Users.

5.7.3.5. Single VoIP Services

Single-Line VoIP Services are all the Hardware, Software and services necessary to provide single-line VoIP Services to End-Users.

5.7.3.6. Multi-Line VoIP Services

Multi-Line VoIP Services are all the Hardware, Software and services necessary to provide multi-line VoIP Services to End-Users.

5.7.3.7. Voice Mail

Voice Mail is an available option to Voices Services upon End-User Service Request or as a stand-alone option available to End-Users without a phone.

The second available option is voice-to-text conversion for Voice Mail. The appropriate E-Mail address receives the converted voice message. This option requires an End-User Service Request.

5.7.3.8. Analog Jack

Analog Jacks are available upon End-User Service Request.

5.7.3.9. [Reserved]

5.7.3.10.Telephone Handsets

Contractor shall own, provision, install, manage, maintain, and support all telephone handsets, including VOIP, with the exclusion of the Microsoft Teams Phone handsets.

5.7.3.11.Virtual Phone

Virtual Phone Services are all the Hardware with the exclusion of the Microsoft Teams Phone handsets., Subcontractor Software, Third Party Software (other than Third Party Software provided by Contractor), and services necessary to provide Virtual Phone Services to End-Users.

5.7.3.12 Virtual Phone Advanced Features

Virtual Phone Services – Advanced Features is an available option to Virtual Phone - Microsoft (MS) Teams Phone and provides auto attendant and call queues. These Advanced Features are only available to MS Teams – Phone subscribers.

5.7.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Voice Services.

Voice Service: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Voice Services solutions that best meets County business requirements.	X	
2. Review and approve recommended Voice Services solutions that best meet County business requirements.		X
3. Produce and submit a VOIP migration plan.	X	
4. Review and approve VOIP migration plan.		X
5. Produce and submit operational plans for Voice Services capacity and performance management.	X	
6. Review and approve operational plans for Voice Services capacity and performance policies and procedures.		X
7. Produce and submit recommendations for Voice Services architecture.	X	
8. Review and approve recommendations for Voice Services architecture.		X
9. Produce and submit Voice Services refresh plan on a yearly basis.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
10. Review and approve Voice Services refresh plan on a yearly basis.		X
11. Produce and submit recommendations for Voice Services migration to current technology.	X	
12. Review and approve recommendations for Voice Services migration to current technology.		X
13. Produce and submit operational policies and procedures for management and support of Voice Services.	X	
14. Review and approve operational policies and procedures for management and support of Voice Services.		X
15. Provide Desk Phone design and engineering to meet County requirements.	X	
16. Approve Desk Phone design and engineering.		X
17. Develop Voice and Web Conferencing Services strategies and requirements.		X
18. Consult on Voice, Web Conferencing Service and Desk Phone strategies with County and actively assist in planning and strategy.	X	
19. Design Voice and Web Conferencing Services to meet County strategies and requirements.	X	
20. Approve Voice and Web Conferencing Services.		X
21. Design and implement customized call flow.	X	
22. Design all queues based on customer requirement that provide Agent mobility.	X	
23. Provide call flow and queue design documentation to each Business Group.	X	
24. Provide consultation to County in developing new or modifying existing ACD applications.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
25. Collaborate with Third-Parties and analyze the following traffic analysis and call reports: • 800 in-bound network traffic summary report • Call detail hourly summary • Call detail traffic summary • Report by each 800 number • Call detail traffic summary by state • Trunk utilization for all trunk groups • Call detail by location • Call completion analysis • Resellers summarized traffic by number • Call prompter summary • Traffic by number and date • Unassigned routing termination number (RTN) • Dial number by RTN	X	
Build Roles and Responsibilities	**Contractor**	**County**
26. Design, test and implement approved Voice Services solutions that best meet County business requirements.	X	
27. Provide least cost routing (LCR) analysis and PBX technology that provides LCR (e.g., "tail end-hop off" LCR methodology).	X	
28. Implement approved operational plans for Voice Services capacity and performance management.	X	
29. Design, test and implement Voice Services architecture.	X	
30. Deploy, manage, communicate and report on activities related to Voice Services refresh.	X	
31. Review and approve Voice refresh report.		X
32. Design, test and implement Voice Services migration to current technology.	X	
33. 33. Install Direct Routing between the O365 Microsoft Teams Tennant and on-premise Avaya Aura infrastructure.	X	
34. Implement approved operational policies and procedures for management and support of Voice Services.		X
Operate Roles and Responsibilities	**Contractor**	**County**
35. Provide support, including break-fix, for all Voice Services Assets.	X	
36. Perform bandwidth management for Voice Services.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
37. Support Voice Services refresh.	X	
38. Support Voice network optimization and traffic engineering.	X	
39. Provide competitive and economically favorable local and long distance rates.	X	
40. Manage and provide end-to-end internal and external phone connectivity including hardware and/or peripherals.	X	
41. Provide Desk Phone requirements (e.g., number of sets, functions and features).		X
42. Assist with set up, troubleshooting, and recommendations on headset options.	X	
43. Provide and maintain End-User Guides, quick reference guides, VoIP training, and End-User Telecom Tips/Q&A for County to publish.	X	
44. Manage PBX systems for class of service according to the authorized County key personnel.	X	
45. Manage the PBX systems to provide least cost routing and tail end hop off for outbound calls.	X	
46. Manage interfaces between PBX network and public carriers.	X	
47. Manage and support Interactive Voice Services.	X	
48. Provide emergency 911 Services to County phones.	X	
49. Provide adaptive voice telecommunications Services and equipment as required by laws affecting the support of the disabled.	X	
50. Manage and maintain private dial plan to be consistent with the County's current dialing method.	X	
51. Provide local and long distance voice Services.	X	
52. Support and manage long distance telephone calling.	X	
53. Provide local and long distance usage monitoring and reporting.	X	
54. Provide and support analog jacks for equipment such as modems, fax machines, or phones.	X	
55. Provide Voice Mail Services.	X	
56. Manage Voice Mail security PBXs, Voice Mail systems, and other Voice Services Assets.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
57. Provide Voice Mail usage monitoring and reporting.	X	
58. Provide Voice Mail storage capacity management.	X	
59. Provide Voice Mail retention management per County requirements and external regulations.	X	
60. Perform Voice Mail mailbox IMARs.	X	
61. Maintain Voice Mail mailboxes configurations by End-User.	X	
62. Provide new Voice Mail End-User training materials.	X	
63. Provide access to voice messages through County E-Mail system.	X	
64. Provide directory Services to the public through a mix of automated and live operators in order to meet call requirements.	X	
65. Provide a secure and searchable online directory service with real time updates (e.g., global directory facility GDF).	X	
66. Provide 411 operator Services for the County which includes a directory of employees, employee locations, departments and telephone numbers.	X	
67. Maintain a directory of County Services for 411 operator Services.	X	
68. Provide 411 operator Services for employee and public inquiries.	X	
69. Update annually telephone numbers.	X	
70. Maintain and update an employee directory website with data from County systems.	X	
71. Maintain business process, systems, and information for phone book and directory assistance in accordance with County approved system design and business processes.	X	
72. Manage local, intrastate, national and international voice teleconferencing Services and support.	X	
73. Provide support for the setup of Voice and Web Conferencing sessions.	X	
74. Create and maintain a monthly and a year-to-date summary report by host, including: conference types, total number of connects, total number of minutes, total call charges, total feature charges, and total charges.	X	

Voice Service: Plan, Build and Operate Roles and Responsibilities		
75. Provide proactive and reactive Voice Services fraud and security management and reporting.	X	
76. Monitor and record all data, such as call rating tables, call usage detail and Move, Add, and Remove orders, generate cost allocation reports for local and long distance usage as well as completed Move, Add and Remove orders.	X	
77. Provide itemized call detail records, including length of each call by telephone number and charge.	X	
78. Provide, maintain and support tollfree (on-net) calls between all County Locations.	X	
79. Provide Casual Use Calling including collect calls, person-to-person calls, person-to-person collect calls, remote calls, operator assistance calls, Third-Party calls, dial one calls, dedicated calls and other miscellaneous calls.	X	
80. Provide Conference Bridge Calls for calls placed to an audio and Web document sharing conference Services that allow multiple people participation and controlled by a unique access code.	X	
81. Provide Directory Assistance Calls for calls placed to obtain a listed telephone directory number.	X	
82. Provide Pay Phones at County Sites for the public's convenience, upon End-User request.	X	
83. Provide an attempted (offered) and handled call volume summary.	X	
84. Provide duration, call transferred and abandoned call reports.	X	
85. Provide PSTN calling for toll free and toll calling as per Exhibit 16.1.1	X	
86. Maintain PSTN calling plan for Microsoft Teams Phone, Single-line Voice and Multi-line Voice RUs as per Exhibit 16.1.1.	X	
87. Operate and maintain Direct Routing between the O365 Microsoft Teams Tennant and on-premise Avaya Aura infrastructure	X	
88. Provide SMS text messaging through IVS applications.	X	
89. Provide IP Conference phones.	X	

5.8. Network Security Services

5.8.1. Overview

The Network Security Services Framework Component of the Network Services Framework includes the Hardware, Software, and services needed to maintain overall network and perimeter security.

Services provided by this Framework Component include, but are not limited to, the following:

- Protection from unauthorized devices, software or users
- Protection from unauthorized access to, or use of, the network and networked assets
- Firewall Services
- Intrusion protection, detection and reporting
- Cloud Access Security Broker (CASB)
- Network Access Control
- Remote Access and Mobile Device Authentication
- Remote Access and Mobile User Authentication
- Data Loss Prevention (DLP)
- Continuous security monitoring, logging and reporting
- Security architecture services
- Data protection
- Prevention of malicious code entry into the network
- Transformational activities to improve the overall security, increase performance and lower costs
- Web content filtering

5.8.2. High Level Requirements

5.8.2.1. Contractor shall develop and maintain a flexible security architecture.

5.8.2.2. Contractor shall provide protection from unauthorized use of, or access to, the County's network and networked resources.

5.8.2.3. Contractor shall control physical access to all Hardware and Software used to provide Network Services.

5.8.2.4. Contractor shall establish secure zones, with County approval, as needed.

5.8.2.5. Contractor shall lock down all Hardware and Software used for Network Services.

5.8.2.6. Contractor shall continuously scan all perimeters and assess vulnerabilities and risk.

5.8.2.7. Contractor shall increase visibility into all data communications and data flows between End-Users and resources within the Data Center or to cloud based services.

5.8.2.8. Contractor shall ensure necessary throughput for perimeter protection and internal security methods that are fast enough to deeply scan and remediate threats at wire speed.

5.8.2.9. Contractor shall implement a "single pane of glass" approach to management and monitoring of Network Security Services.

5.8.2.10. Contractor shall provide management, refresh, support, reporting and logging of all firewalls used in the delivery of the Services.

5.8.2.11. Contractor shall provide information event logging, analysis, reporting and management of all Hardware and Software used to provide Network Security Services.

5.8.2.12. Contractor shall provide intrusion detection and prevention systems.

5.8.2.13. Contractor shall provide unified threat management.

5.8.2.14. Contractor shall update all Hardware and Software used for Network Security Services to the latest patch, service packs, or other updates promptly to ensure operational integrity.

5.8.2.15. Contractor shall refresh all Hardware and Software used for Network Security Services on a 4-year cycle unless otherwise approved by the County.

5.8.2.16. Contractor shall maintain all Hardware used in the delivery of Network Security Services to maximize performance with high-speed network operations.

5.8.2.17. Contractor shall continuously identify and correct, with County approval, any single point failures within the Network Security Services.

5.8.2.18. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Network Security Services.

5.8.2.19. Contractor shall continuously maintain a timeline/roadmap of all Network Security Services Hardware and Software life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

5.8.2.20. Contractor shall provide a cloud-based CASB service that will enforce County security policy on County SaaS data. This will include enforcement of DLP policies, enforcement of collaboration policies, capture of audit trails for forensic use, detection of compromised accounts and other threats, and other features that further extend the County security protection.

5.8.3. Environment

The following further describe and scope Network Security Services elements supported by Contractor and with which Contractor shall comply.

5.8.3.1. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Network Security Services

5.8.3.2. Technology Refresh

Contractor shall refresh Network Security Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.8.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Network Security Services.

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Security architecture.	X	
2. Review and approve recommendations for Security architecture.		X
3. Produce and submit plans for monitoring and managing access to the County Intranet.	X	
4. Review and approve plans for monitoring and managing access to the County Intranet.		X
5. Produce and submit plans that provide security to physical and logical devices connected to the network.	X	
6. Review and approve plans to include the provision and support of methods that provide security to physical and logical devices connected to the network.		X
7. Produce and submit recommendations on firewall policies that comply with County policy.	X	
8. Review, approve and identify firewall policies that comply with County policy.		X
9. Perform firewall engineering and firewall security design	X	
10. Assess firewall security and propose alternative security designs.	X	
11. Review and approve firewall security designs.		X
12. Produce and submit recommendation of Network Security Services Assets refresh or upgrade plan on a yearly basis.	X	
13. Review and approve recommendations on Network Security Services Assets refresh or upgrade plan.		X

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
14. Produce and submit recommendations for improved network security.	X	
15. Review and approve recommendations for improved network security.		X
16. Produce and submit recommendation of policies for security vulnerability and penetration testing.	X	
17. Review and approve policies for security vulnerability and penetration testing.		X
18. Produce and submit plans for Network Security Services asset updates or patches.	X	
19. Review and approve plans for Network Security Services asset updates or patches.		X
Build Roles and Responsibilities	**Contractor**	**County**
20. Design, test and implement approved Network Security architecture.	X	
21. Design and implement monitoring and managing access plans as approved.	X	
22. Design, test and implement plans to secure network attached devices.	X	
23. Design, test and implement approved firewall policies.	X	
24. Design, test, implement and report Network Security Services Assets refresh or upgrade.	X	
25. Review and approve reports for Network Security Services Assets refresh or upgrade.		X
26. Design and implement approved recommendations for improving network security.	X	
27. Design and implement approved policies for security vulnerability and penetration testing.	X	
28. Design, test and implement updates or patches approved for Network Security Services Assets.	X	
29. Design a centralized authentication database for remote County employees, Third-Party and agents using VPN and deploy new systems interfacing with single-sign-on authentication Services.	X	

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
30. Deploy a Security Information Management System (SIMS) for aggregation and centralization of Incident alerts and correlation and provide SIMS information to the County through online access.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
31. Provide support, including break-fix, for all Security Services Assets.	X	
32. Provide 24/7/365 security monitoring Services including a Security Operations Center (SOC), IDS/IPS infrastructure and intranet/Internet firewalls.	X	
33. Provide services in conformance to firewall policies and requirements.	X	
34. Provide reporting on security testing results.	X	
35. Provide initial review of security Incidents and the determination if escalation, including to County Information Security, is warranted.	X	
36. Provide standardized End-User operations and also custom reports regardless of the End-User's location and/or department.	X	
37. Identify and remove from the network any malicious-code infected System.	X	
38. Identify and provide countermeasures for malicious code attacks (i.e., both prevention and remediation).	X	
39. Block unauthorized party access and provide notification of unauthorized access attempts.	X	
40. Encrypt (and prioritize) all County traffic that uses public MPLS network transport facilities (such as OPT-E-MAN or DSL) through the engineering and implementation of generic routing encapsulation (GRE) VPN tunnels (e.g., 256-bit Advanced Encryption Standard (AES) key).	X	
41. Provide technical expertise for security reviews.	X	
42. Collect all logs and review all Incidents reported by all other security Services (e.g., NIPS, HIPS, penetration testing, and firewall).	X	
43. Maintain log files in accordance with County policies and Service Levels.	X	

Network Security Service: Plan, Build and Operate Roles and Responsibilities		
44. Provide security reporting.	X	
45. Provide fraud prevention, detection and reporting.	X	
46. Provide, control, monitor, and maintain security encryption interface at the data network level.	X	
47. Provide security devices on supported PBXs, Voice Mail systems, and other appropriate adjunct remote administration ports.	X	
48. Implement security violation notification.	X	
49. Conduct security perimeter vulnerability assessments and annual penetration testing.	X	
50. Provide Cloud Access Security Broker (CASB) capability.	X	
51. Provide CASB reporting.	X	
52. Provide CASB connectivity to Contractor SIEM service.	X	

5.9. Video Conferencing Services

5.9.1. Overview

Video Conferencing Services Framework Component of the Network Services Framework consists of the activities and functions of providing two-way video transmission between different entities within the County as well as outside of the County.

Services provided by this Framework Component include, but are not limited to, the following:

- Enable closed-circuit video conference
- Point-to-point communications within County network connected Sites
- Point-to-point to external State or Federal facilities
- Multi-point hosting of meetings
- Desktop integration into Video Conferencing Services
- External multi-point integration into Video Conferencing Services
- Develop two types of Video Conferencing systems: room and personal.

5.9.2. High Level Requirements

5.9.2.1. Contractor shall provide a reliable and secure Video Conferencing Services that enables County End-Users and authorized external Users to participate.

5.9.2.2. Contractor shall identify and correct, with County approval, any single point failures with Video Conferencing Services.

5.9.2.3. Contractor shall integrate Unified Communications Services into Video Conferencing Services.

5.9.2.4. Contractor shall plan and implement, as requested by the County, Town Hall Services for internal County use.

5.9.2.5. Contractor shall apply County approved security policies to all Video Conferencing Services hardware, software and services.

5.9.2.6. Contractor shall provide End-User authentication, as needed, for all Video Conferencing Services.

5.9.2.7. Contractor shall continuously provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Video Conferencing Services.

5.9.2.8. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Video Conferencing Services.

5.9.2.9. Contractor shall continuously develop, update and maintain help desk scripts and processes for Video Conferencing Services End-User support.

5.9.3. Environment

The following further describe and scope Video Conferencing Services elements supported by Contractor and with which Contractor shall comply.

5.9.3.1. Hardware and Software

Contractor shall own, provision, install, manage, maintain, and support all Hardware, Software, licenses, tools needed in the delivery of Video Conferencing Services

5.9.3.2. Technology Refresh

Contractor shall refresh Video Conferencing Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.9.4. Roles and Responsibilities

The following table identifies the roles and responsibilities associated with Video Conferencing Services.

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for video conferencing standards annually.	X	
2. Review and approve recommendations for video conferencing standards.		X
3. Publish video conferencing standards in the Standards and Procedures Manual on the Service Portal.	X	
4. Produce and submit plans for new, replacement and upgrades to Video Conferencing Services.	X	
5. Produce and submit plans for infrastructure systems (Gatekeeper and Border Controller) and network capacities to support IP based VTC systems.	X	
6. Review and approve plans for new, replacement and upgrades to Video Conferencing Services, infrastructure/network systems.		X
7. Provide Project Management for the installation of new VTC systems.	X	
8. Conduct site review to determine the installation time period (the installation interval is targeted to be 30 days or less, the actual installation period shall be determined after a site review is conducted for that particular system).	X	

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
9. Review and approve site review report.		X
10. Make recommendations to the County for new Video Conferencing Services strategy as new devices, infrastructures and protocols emerge.	X	
11. Review and approve recommendations for new Video Conferencing Services strategy as new devices, infrastructures and protocols emerge.		X
12. Provide a selection of Video Conferencing Services optional items via the OIC.	X	
13. Select Video Conferencing Services optional items via the OIC.		X
Build Roles and Responsibilities	**Contractor**	**County**
14. Design and implement new, replacement or upgrades to Video Conferencing Services.	X	
15. Design and implement infrastructure systems to support IP based VTC systems.	X	
16. Review and approve design changes and implementation plans to Video Conferencing Services, infrastructure and network systems/circuits.		X
17. Provide infrastructure systems that monitors and maintains the QOS of the IP network (Gatekeeper) and supports secure off-net IP based video conferences (Border Controller).	X	
18. Provide basic installation which includes the assembly and placement of any furniture (roll-about cart), component or option provided as part of the new VTC system; along with the placement, connecting, configuration and testing of any electronics provided as part of the new VTC system and any other activities.	X	
19. Review and approve the installation activities.		X
20. Test and deploy approved changes to Video Conferencing Services including infrastructure systems and network Services.	X	
21. Develop and provide training related to the implementation of new products and Services.	X	
22. Provide training to County department personnel for proper operation of hardware and software components and scheduling tool.	X	

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
23. Provide network access to new systems by trained and qualified video engineers and technicians to enable remote diagnostics and efficient triage of trouble reports.	X	
24. Provide Users access to the VTC Third-Party Supplier's management system scheduling tool so that County End-Users can schedule their own video conferences.	X	
25. Provide project management including coordinating with and providing support to Third-Party.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
26. Provide support and maintenance, including break-fix, for new Video Conferencing Services, and limited break-fix for legacy Video Conferencing Systems (excluding parts replacement for legacy Video Conferencing Systems).	X	
27. Provide IMAR Services.	X	
28. Provide and support infrastructure Services for point-to-point, multipoint video conferencing, and Presentation features, Quality of Service and on-net/off-net video conferencing security.	X	
29. Support Video Conferencing Assets.	X	
30. Provide point-to-point, multi-point and ISDN to IP video conferencing Services to the County, both inside and outside the County's network.	X	
31. Provide and maintain the network security infrastructure to support external video conferences for all County departments.	X	
32. Provide video bridging service for County's use to facilitate IP and multipoint video conferences.	X	
33. Provide single point of contact for Incident call handling.	X	
34. Provide access to manufacturer's customer service technical support center to assist County End-Users on equipment operation and any other questions they may have about the systems.	X	
35. Provide software patches and version updates as recommended by equipment for Video Conferencing Services Assets.	X	
36. Provide parts and device warranty, repair and/or parts replacement of all components for systems of Video Conferencing Services.	X	

Video Conferencing Services: Plan, Build and Operate Roles and Responsibilities		
37. Provide multi-cast record/archive service.	X	
38. Integrate teleconferencing into video conference meetings upon request.	X	
39. Monitor and support calls in progress.	X	
40. Maintain and manage video conference calendar and scheduling.	X	
41. Manage and maintain video room calendar and coordinate reservations.	X	
42. Provide miscellaneous video support and advice as required by County.	X	
43. Provide video conferencing service support through County Service Desk.	X	

5.10. Video Streaming and Archiving Services

5.10.1. Overview

This section pertains to the Video Streaming and Archiving Services Framework Component within the Network Services Framework.

Services provided by this Framework Component include, but are not limited to, the following:

- providing live or archived video data or content via a web page to the County Intranet or the external public
- archiving such video data or content to be available for public viewing for one year

County currently uses Granicus Services to provide the Video Streaming and Archiving Services.

5.10.2. High Level Requirements

5.10.2.1. Contractor shall provide and maintain live video streaming broadcast, of Board of Supervisors meetings, over the Internet to worldwide audiences and to End-Users.

5.10.2.2. Contractor shall deliver and distribute video streaming broadcasts of high quality video to all End-Users.

5.10.2.3. Contractor shall provide and maintain video streaming across the County network.

5.10.2.4. Contractor shall optimize Video Streaming and Archiving Services across the County network to maximize End-User performance.

5.10.2.5. Contractor shall identify and correct and single point issues with the Video Streaming and Archiving Services to ensure maximum reliability and performance.

5.10.2.6. Contractor shall archive video streamed broadcasts and store such archives for twelve months and provide public access, via the Internet, to and viewing of such archives.

5.10.2.7. Contractor shall provide the Board of Supervisors with a solution to automate and easily manage the entire legislative process. In particular this solution will allow the elected officials to submit Board Letters, compiling and generating agendas, and creating Minute Orders.

5.10.2.8. Contractor shall provide a web-based service to collect feedback from citizens on specific items associated with upcoming Board of Supervisor's meetings. Contractor shall also provide an online solution that promotes and facilitates community engagement by allowing constituents to share opinions, submit questions, create polls and surveys.

5.10.2.9. Contractor shall provide a custom web page for collecting the feedback and such web page activated by a link dropped on the County's existing Board of Supervisors agenda page.

5.10.2.10. Contractor shall provide a touch-voting solution to the Board of Supervisors, which will include the following functionalities:

5.10.2.10.1. Real-time meeting voting and recording via touch-screen device such as the VoteCast Classic and an iPad or Android voting machine.

5.10.2.10.2. Viewing of full agendas and supporting materials via touch-screen.

5.10.2.11. Elected officials can make or second a motion, cast a vote, review previously cast votes, and request to speak on items using touch-screen devices.

5.10.2.12. Contractor will provide hosting services sufficient to enable use of, and access to, the application. Contractor will also provide maintenance and support of all hardware, firmware, software, and telecommunications equipment and facilities necessary for the delivery of the services.

5.10.2.13. Contractor shall continuously provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Video Streaming and Archiving Services.

5.10.2.14. Contractor shall continuously develop and update training documentation and End-User tip sheets and post on the Service Portal for County End-Users on the use of Video Streaming and Archiving Services.

5.10.2.15. Contractor shall continuously develop, update and maintain help desk scripts and processes for Video Streaming and Archiving Services End-User support.

5.10.3. Environment

The following further describe and scope Video Streaming and Archiving Services elements supported by Contractor and with which Contractor shall comply.

5.10.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Video Streaming and Archiving Services.

5.10.3.2. Technology Refresh

Contractor shall refresh Video Streaming and Archiving Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.10.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Video Streaming and Archiving Services.

Video Streaming and Archiving Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit annual plans and recommendations for new, replacement and upgrades to Streaming and Archiving Services based on market evaluation and emerging technologies.	X	
2. Review and approve annual plans and recommendations		X
Operate Roles and Responsibilities	**Contractor**	**County**
3. Provide support, including break-fix, for Video Streaming and Archiving Services.	X	
4. Provide and maintain internet video and audio streaming broadcasts, including broadcasts of Board of Supervisors meetings.	X	
5. Provide archiving and public viewing and retrieval of broadcasts of Board of Supervisors meetings for twelve (12) months following the date of such meetings.	X	
6. Provide broadcast feed of County of San Diego Board of Supervisors meetings to the Cox (or the applicable successor) cable television distribution network.	X	

5.11. Mobility Infrastructure Services

5.11.1. Overview

This section pertains to the Mobility Infrastructure Services Framework Component within the Network Services Framework.

Services provided by this Framework Component include, but are not limited to, the following:

- Mobile device management

- Centralized mobile device management platform
- Manage mobile device configurations
- Provision device security policies
- Mobile device authentication services
- Mobile application store
- Application gateways
- Mobile VPN services

5.11.2. High Level Requirements

5.11.2.1. Contractor shall provide a reliable and secure Mobility Infrastructure Services for mobile County End-Users and authorized bring your own device (BYOD) Users.

5.11.2.2. Contractor shall design, deliver, for County approval, and implement a mobile device management platform.

5.11.2.3. Contractor shall continuously identify and correct, with County approval, any single point failures with Mobility Infrastructure Services.

5.11.2.4. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Mobile Infrastructure Services.

5.11.2.5. Contractor shall enable the central management and control all mobile devices (including BYOD), platforms and applications from a single unified console.

5.11.2.6. Contractor shall implement, County approved, device policies for security and data protection using the Mobility Infrastructure Services on all mobile devices (including BYOD).

5.11.2.7. Contractor shall deploy and manage developed or acquired mobile applications within the Mobility Infrastructure Services application store.

5.11.2.8. Contractor shall provide continuous updated documentation that details operation and use Mobility Infrastructure Services and post them on the Service Portal.

5.11.2.9. Contractor shall recommend, for County approval, standards on a yearly basis for all Mobility Infrastructure Services.

5.11.2.10. Contractor shall recommend, for County approval, mobile devices standards including hardware and operating system.

5.11.2.11. Contractor shall facilitate and enable application gateways services for developed or acquired applications, with County approval, to internal County resources from mobile devices using Mobility Infrastructure Services.

5.11.2.12. Contractor shall maintain a continuous timeline/roadmap of all Mobility Infrastructure Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

5.11.2.13. Contractor shall reference the Standards and Procedures manual for standard Mobile Devices to be supported.

5.11.3. Environment

The following further describe and scope Mobility Infrastructure Services elements supported by Contractor and with which Contractor shall comply.

5.11.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Mobility Infrastructure Services.

5.11.3.2. Technology Refresh

Contractor shall refresh Mobility Infrastructure Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.11.4. Roles and Responsibilities

The following table identifies the roles and responsibilities associated with Mobility Services.

Mobility Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Provide centralized, secure Mobile Device Management and Support Services for iOS, Android and Windows Phone devices (smartphones or tablets).	X	
2. Perform management and support of mobile devices management application including MDM application updates, configuration and troubleshooting, point releases and fixes as required.	X	
3. Maintain certificates and password resets as required	X	
4. Perform and provide over-the-air (OTA) self-provisioning, policy setting on device and connection configuration, including the ability to set encryption, VPN configuration and Wi-Fi settings with verification to streamline activations and eliminate the need for IT involvement.	X	
5. Provide an Enterprise Mobile Device Application store which can be used for application publishing to devices, through a push by User group (labor for the creation or modification of applications for the Application Store shall be provided through Application Service Requests). The Application Store accessed from all supported devices.	X	
6. Perform and submit operational planning for Mobile Device Management and Support capacity and performance purposes.	X	
7. Review and approve operational planning for Mobile Device Management and Support capacity and performance purposes.		X
8. Design operational views and status reports for the Service Portal.	X	
9. Review and approve operational views and status reports.		X
10. Design operational reports per County request.	X	
11. Review and approve operational reports.		X
12. Produce and submit Mobile Device Management and Support operational policies and procedures including escalation.	X	

Mobility Services Roles and Responsibilities		
13. Review and approve Mobile Device Management and Support operational policies and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
14. Develop and improve Mobile Device Management and Support build as appropriate to improve performance.	X	
15. Provide all test Services and produce documentation required to support Mobile Device Management and Support Services.	X	
16. Produce and submit all test documentation to County.	X	
17. Review and approve all test documentation.		X
18. Provide all deployment Services required to support Mobile Device Management and Support Services.	X	
19. Produce and submit to County all Mobile Device Management and Support Services deployment documentation.	X	
20. Review and approve all Mobile Device Management and Support Services deployment documentation.		X
21. Produce and submit plans to apply Mobile Device Management and Support Services application releases and patches as required.	X	
22. Review and approve Mobile Device Management and Support Services application releases and patches plans.		X
23. Enforce security to continuously review all connected devices and quarantine or revoke service for unmanaged or compromised devices.	X	
24. Deliver simplification of mobile application deployment with an enterprise-specific over-the-air (OTA) catalog of mandatory, recommended and available applications, without requiring the use of a commercial Application Store such as Google Play or iTunes Store.	X	

Mobility Services Roles and Responsibilities		
25. Provide security management, including the general functionality described in this Resource Unit. The specific settings are defined by County policy as: • Require passcode • Wipe device after too many passcode attempts • Restrict/Permit applications • Restrict/Permit content • Enforce application blacklist/whitelist • Manage device configurations • Manage Exchange and Active sync E-Mail configurations • Provide the ability to manage application sets and tie them to Active Directory • In the event of lost or stolen assets, the asset shall be wiped of all County Data	X	
Operate Roles and Responsibilities	**Contractor**	**County**
26. Perform routine database maintenance and backups to maintain optimal performance of the Mobile Device Management and Support Services Platform.	X	
27. Maintain the Mobile Device Management and Support Services Platform configuration per engineering build documents and County policy.	X	
28. Maintain all Mobile Device Management and Support Services certificates for the platform and the devices.	X	
29. Perform all device specified Services through the Mobile Device Management and Support Services console (e.g., remote wipes and password resets).	X	
30. Provide continuous monitoring of all connected devices for security Incidents.	X	
31. Quarantine or revoke service for any unmanaged or compromised mobile device.	X	
32. Manage mobile devices through Active Directory group membership.	X	
33. Manage County approved BYOD devices to specific applications authorized by the County.	X	
34. Utilize the Service Portal to monitor system performance.	X	
35. Provide operational reports as requested.	X	

Mobility Services Roles and Responsibilities		
36. Manage Enterprise Application Store to add and delete mobile applications.	X	
37. Provide security protection to maintain control of County information and selectively wipe only County Data and applications, or all data, from managed devices with review of successful completion.	X	
38. Provide County required reporting on Mobile devices usage, billing and invoicing Services.	X	
39. Coordinate between User, Service Desk and Third-Parties such as Mobile/Wireless Carrier or device manufacturer to manage all User and device related Incidents and Service Requests as needed.	X	
40. Provide a single point of contact for the mobile device environment including coordination with Third-Parties as needed.	X	
41. Provide ability to securely access authorized enterprise content from any authorized mobile device.	X	
42. Provide ability to enforce County security and policy through role-based models.	X	
43. Provide for personal and corporate data to securely coexist on the same device.	X	
44. Enable employee self-activation of corporate and personal devices.	X	
45. Provide authorized End-Users access to Service Portal.	X	
46. Provide the ability to monitor device usage and enforce security from a single global console.	X	
47. Provide Services to secure data, applications, communication, and network access from authorized mobile devices.	X	
48. Pre-configure device settings and policies based on ownership models.	X	
49. Provide Services that protect devices from unauthorized use.	X	
50. Provide ability to control specific device features and applications.	X	
51. Provide the ability to enforce authorized Wi-Fi and VPN networks on mobile devices.	X	

Mobility Services Roles and Responsibilities		
52. Provide Services to secure devices, data, applications, communication, and network access.	X	
53. Provide Services that implement secure data leakage prevention.	X	
54. Provide Services that protect against malware and unauthorized access via custom profiles.	X	
55. Support County in performing security and compliance reviews on mobile devices as needed.	X	

5.12. Wireless Network Access Services

5.12.1. Overview

This section pertains to the Wireless Network Access Services Framework Component within the Network Services Framework. The Wireless Network Access Services Framework Component applies to the Wireless Local Area Network (WLAN) located throughout various County Sites. The WLAN allows County End-Users and authorized users to establish a secure connection to the County internal network or an unsecured connection, taken directly to the Internet, for visitors.

Services provided within this Framework Component include, but are not limited to, the following:

- Accessibility to County resources for wireless connected End-Users
- Security from unauthorized users
- Central management of Wireless Network Access Hardware and Software
- Performance better or equal to wired network for secure network access
- Secure network integration
- Network access control
- Network capacity and performance monitoring
- Network engineering
- Transformational activities to improve overall service
- Technical refresh

5.12.2. High Level Requirements

5.12.2.1. Contractor shall maintain technical currency on Wireless Network Access Services Hardware and Software.

5.12.2.2. Contractor shall ensure that all devices attached to the secure network WLAN are valid and authorized.

5.12.2.3. Contractor shall continuously identify and correct, with County approval, any single point failures within the Wireless Network Access Services.

5.12.2.4. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Wireless Network Access Services.

5.12.2.5. Contractor shall deploy WLAN to the secured network for all County authorized, wireless End-Users using appropriate device and user authentication.

5.12.2.6. Contractor shall deploy WLAN to the unsecured network for all County visitors.

5.12.2.7. Contractor shall provide End-User authentication for all interaction with the secure WLAN.

5.12.2.8. Contractor shall deploy device authentication for secure WLAN access using County PKI infrastructure.

5.12.2.9. Contractor shall ensure that the Wireless Network Access Services network is secure by implementing County security policies and using Network Access Control.

5.12.2.10. Contractor shall deploy a guest access portal and splash screen to unsecured WLAN for County visitors.

5.12.2.11. Contractor shall make available two types of Wireless Access Points interior mounted and exterior mounted.

5.12.2.12. Contractor shall continuously maintain a timeline/roadmap of all Wireless Network Access Services Hardware and Software life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

5.12.3. Environment

The following further describe and scope Wireless Network Access Services elements supported by Contractor and with which Contractor shall comply.

5.12.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Wireless Network Access Services.

5.12.3.2. Technology Refresh

Contractor shall refresh Wireless Network Access Services Wireless Access Points (WAPs) on a 3-year refresh schedule and all other Wireless Network Access Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.12.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Wireless Network Access Services.

Wireless Network Access Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendation for Wireless Network Access Services architecture.	X	
2. Review and approve Wireless Network Access Services architecture.		X

Wireless Network Access Services Roles and Responsibilities		
3. Produce and submit Wireless Network Access Services refresh plan on a yearly basis.	X	
4. Review and approve Wireless Network Access Services refresh plan on a yearly basis.		X
5. Produce and submit Wireless Network Access Services policies and procedures.	X	
6. Review and approve Wireless Network Access Services policies and procedures.		X
7. Produce and submit Wireless Network Access Services security architecture.	X	
8. Review and approve Wireless Network Access Services security architecture.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Design, test and implement approved Wireless Network Access Services architecture.	X	
10. Deploy, manage, communicate and report on activities related to Wireless Network Access Services refresh.	X	
11. Review and approve Wireless Network Access Services refresh report.		X
12. Develop and implement Wireless Network Access Services policies and procedures.	X	
13. Design, test and implement approved Wireless Network Access Services architecture.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Provide support, including break-fix, for all Wireless Network Access Services Assets.	X	

5.13. Third-Party Network Access Services

5.13.1. Overview

This section pertains to the Third-Party Network Access Services Framework Component within the Network Services. The Third-Party Network Access Services Framework Component applies to security services, network transport and bandwidth required for Third-Party access to the County network.

Services provided within this Framework Component include, but are not limited to, the following:

- Protection from unauthorized network access
- Firewall services
- Intrusion protection
- Detection and reporting
- Security monitoring
- Data protection
- Network management
- Network capacity and performance monitoring
- Third-Party network to County network connectivity
- User authentication services

5.13.2. High Level Requirements

5.13.2.1. Contractor shall establish and maintain Third-Party Network Access Services to the County secure network.

5.13.2.2. Contractor shall monitor, log and report all activity related to Third-Party Network Access Services.

5.13.2.3. Contractor shall ensure necessary bandwidth and capacity are in place for all Third-Party Network Access Services.

5.13.2.4. Contractor shall ensure all appropriate County security policies are in place and that the County secure network is maintained as safe from compromise.

5.13.2.5. Contractor shall identify and correct, with County approval, any single point failures with Third-Party Network Access Services.

5.13.2.6. Contractor shall provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Third-Party Network Access Services.

5.13.3. Environment

The following describes the scope for Third-Party Network Access Services elements supported by Contractor.

5.13.3.1.Hardware and Software

Contractor shall provide all Hardware and Software to support Third-Party Network Access Services.

5.13.3.2.Technology Refresh

Contractor shall refresh Third-Party Network Access Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.13.3.3.Security Services

Security Services include all the Hardware, Software, and services to ensure secure and authorized access to the County secure network

5.13.3.4.Network Services

Network Services include all the Hardware, Software, and services needed by a Third-Party access to the County secure network. The three (3) categories are private network circuits or connections, Private Circuit/Connection, IPSEC Tunnels and Virtual Access Connections. The circuit connecting to the County is the responsibility of the Third-Party.

5.13.3.4.1. Private Circuit/Connection

- Category 1 — any circuit or connection less than T1 speed (1.544mbps)
- Category 2 — any circuit or connection equal to T1 speed
- Category 3 — any circuit or connection greater than T1 speed

5.13.3.4.2. IPSEC Tunnels Connection

- IPSEC Tunnel 5Mbs
- IPSEC Tunnel 10Mbs

5.13.3.4.3. Virtual Access Connection

- Virtual Access 1Mbps
- Virtual Access 2Mbps
- Virtual Access 3Mbps
- Virtual Access 4Mbps
- Virtual Access 5Mbps
- Virtual Access 5Mbps – Microsoft Teams Rooms (MTR)
- Virtual Access 10Mbps
- Virtual Access 20Mbps
- Virtual Access 30Mbps
- Virtual Access 40Mbps
- Virtual Access 50Mbps

5.13.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Third-Party Network Access Services.

Third-Party Network Access Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Third-Party Network Access Services architecture.	X	
2. Review and approve recommendations for Third-Party Network Access Services architecture.		X
3. Produce and submit plans for monitoring and managing access to the County network from Third-Party entities.	X	
4. Review and approve plans for monitoring and managing access to the County network from Third-Party entities.		X
5. Produce and submit recommendations on firewall policies that comply with County policy.	X	
6. Review and approve firewall policies.		X
7. Produce and submit recommendation of Third-Party Network Access Services Assets refresh or upgrade plan on a yearly basis.	X	
8. Review and approve recommendations on Third-Party Network Access Services Assets refresh or upgrade plan.		X

Third-Party Network Access Services Roles and Responsibilities		
9. Produce and submit plans for Third-Party Network Access Services Asset updates or patches.	X	
10. Review and approve plans for Third-Party Network Access Services Asset updates or patches.		X
Build Roles and Responsibilities	**Contractor**	**County**
11. Design, test and implement approved Third-Party Network Access Services architecture.	X	
12. Design and implement monitoring and managing access plans as approved.	X	
13. Design, test and implement approved firewall policies.	X	
14. Design, test, implement and report Third-Party Network Access Services Assets refresh or upgrade.	X	
15. Review and approve reports for Third-Party Network Access Services Assets refresh or upgrade.		X
16. Design, test and implement updates or patches approved for Third-Party Network Access Services Assets.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
17. Provide support, including break-fix, for all Third-Party Network Access Services Assets.	X	
18. Provide services in conformance to firewall policies and requirements.	X	
19. Support Third-Party Network Access Services refresh.	X	
20. Manage network interfaces between the County and Third-Parties.	X	
21. Produce and submit network utilization, capacity and performance reports.	X	
22. Provide initial review of security Incidents and the determination if escalation, including to County Information Security, is warranted.	X	
23. Provide standardized End-User operations and also custom reports regardless of the End-user's location and/or department.	X	
24. Identify and remove from the network any malicious-code (malware) infected System.	X	

Third-Party Network Access Services Roles and Responsibilities		
25. Identify and provide countermeasures for malware attacks (i.e., both prevention and remediation).	X	
26. Collect all logs and review all Incidents reported by all other security Services (e.g., NIPS, HIPS, penetration testing, and firewall).	X	
27. Maintain log files in accordance with County policies and Service Levels.	X	
28. Provide security reporting.	X	
29. Provide fraud prevention, detection and reporting.	X	

5.14. External DNS Management Services

5.14.1. Overview

This section pertains to the External DNS Management Services Framework Component within the Network Services Framework. The External DNS Management Services Framework Component applies to a cloud-based DNS solution that is available 24/7/365.

Services provided within this Framework Component include, but are not limited to, 24/7/365 DNS availability, improved DNS responsiveness, Web Application Firewall, Geo blocking, Security Monitor, Client Reputation, IP Whitelists / Blacklists, Bot Management, Dynamic Site Accelerator (CDN), defense against DDoS or similar type attacks, distributed Anycast network, primary and secondary DNS services and interface to internal DNS services.

Akamai Fast DNS Service along with Kona Security Service and Bot Management Service are used to provide External DNS Management Services.

5.14.2. High Level Requirements

5.14.2.1. Contractor shall leverage current Akamai Fast DNS Service for External DNS Management Services.

5.14.2.2. Contractor shall support and manage all aspects of External DNS Services including integration to internal DNS services, as needed.

5.14.2.3. Contractor shall maintain DNS to reduce orphan or bad records.

5.14.2.4. Contractor shall continuously identify and correct, with County approval, any single point failures within the External DNS Management Services.

5.14.2.5. Contractor shall facilitate a quarterly meeting with Akamai, Contractor resources and County to review roadmaps, support status and emerging services.

5.14.2.6. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to External DNS Management Services.

5.14.2.7. Contractor shall leverage "Web Application Firewall" component from Kona Security Services to inspect application traffic and block suspicious or known exploits.

5.14.2.8. Contractor shall leverage "Geo Blocking" component from Kona Security Services to block traffic originating from specific geographical locations.

5.14.2.9. Contractor shall leverage "Security Monitor" component from Kona Security Services to provide real-time visibility into network- and application-layer attacks.

5.14.2.10. Contractor shall leverage "Client Reputation" component from Kona Security Services to block attackers proactively when they're detected elsewhere on the Akamai Platform.

5.14.2.11. Contractor shall leverage "IP Whitelists / Blacklists" component from Kona Security Services to define list of IP addresses to allow or block for positive and negative security.

5.14.2.12. Contractor shall leverage "Bot Manager Standard" from Akamai to identify and manage bots targeting the County websites.

5.14.2.13. Contractor shall continuously maintain a timeline/roadmap of all External DNS Management Services Hardware and Software life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

5.14.3. Environment

The following further describe and scope External DNS Management Services elements supported by Contractor and with which Contractor shall comply.

5.14.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support External DNS Management Services.

5.14.3.2. External Service

Contractor shall own and manage all contracts with cloud based Third-Parties supporting External DNS Management Services.

5.14.3.3. Technology Refresh

Contractor shall refresh External DNS Management Services Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

Excluded from technology refresh are all cloud based External DNS Management Services. Cloud based Third-Parties update per product release cycles.

5.14.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with External DNS Management Services.

External DNS Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a solution design on External DNS Services.	X	

External DNS Management Services Roles and Responsibilities		
2. Review and approve the solution design for External DNS Services.		X
3. Produce and submit External DNS Services operational procedures.	X	
4. Review and approve External DNS Services operational procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Produce and maintain an authoritative record of externally-visible County services and of internally-visible County services.	X	
6. Produce and maintain an authoritative record of the County's public network address ranges and the physical networks.	X	
7. Develop and submit a continuously emerging architecture to ensure that External DNS Services are highly available during normal operations and that they failover during any unplanned event.	X	
8. Review and approve External DNS documentation and technical architecture.		X
Operate Roles and Responsibilities	**Contractor**	**County**
9. Configure and maintain External DNS Services.	X	
10. Configure and maintain DNS records on external DNS Services provided by Akamai.	X	
11. Maintain domain names for External DNS.	X	
12. Submit any recommended changes to External DNS records for County approval.	X	
13. Review any proposed changes to External DNS records.		X
14. Produce monthly reports showing External DNS records and domains.	X	

5.15. IP Address Management Services

5.15.1. Overview

This section pertains to the IP Address Management Services Framework Component within the Network Services Framework. The IP Address Management Services

Framework Component applies to the single console management of all IPv6 addresses and all IPv4 public and private addresses within the County network.

5.15.2. High Level Requirements

5.15.2.1. Contractor shall allocate IPv4 and IPv6 address ranges within the County.

5.15.2.2. Contractor shall provide Internet routing to all IP address ranges assigned unless otherwise approved by the County Contractor shall provide robust reporting capability that enables detailed tracking of IP address utilization trends.

5.15.2.3. Contractor shall implement and allocate fixed and dynamic IP addresses to the appropriate network-attached device.

5.15.2.4. Contractor shall assign and maintain IP address ranges for all County Locations.

5.15.2.5. Contractor shall provide integrated management of dynamic and static IP address space.

5.15.2.6. Contractor shall provide detection and management of conflicts, overlaps, and duplicates in address space.

5.15.2.7. Contractor shall provide automated discovery of IP address ranges from DHCP scopes.

5.15.2.8. Contractor shall provide continuous synchronization with internal DNS services.

5.15.2.9. Contractor shall provide continuous alignment with Active Directory "Sites and Services" for all in use IP Address ranges.

5.15.2.10. Contractor shall continuously identify and correct, with County approval, any single point failures within the IP Address Management Services.

5.15.2.11. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to IP Address Management Services.

5.15.2.12. Contractor shall continuously maintain a timeline/roadmap of all IP Address Management Services Hardware and Software life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

5.15.3. Environment

The following further describe and scope IP Address Management Services elements supported by Contractor and with which Contractor shall comply.

5.15.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support IP Address Management Services.

5.15.3.2. Technology Refresh

Contractor shall refresh IP Address Management Hardware and Software on a 4-year refresh schedule unless otherwise agreed by the County in writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.15.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with IP Address Management Services.

IP Address Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a documentation p allocation of network address ranges for new networks, the assignment of addresses and device names for new servers for DHCP Services.	X	

IP Address Management Services Roles and Responsibilities		
2. Identify an IP Address Management (IPAM) tool that is used for managing and reporting IP address allocations and DHCP configurations.	X	
3. Review and approve an IPAM tool that is used for managing and reporting IP address allocations and DHCP configurations.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Produce and submit IP Address Management design to ensure that DHCP Services are highly available during normal operations and that they failover during any unplanned event.	X	
5. Review and approve IP Address Management design.		X
6. Implement IP Address Management design.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Allocate network address ranges for new networks and assign addresses.	X	
8. Submit any recommended changes to DHCP configuration for County approval.	X	
9. Review and approve any proposed changes to DHCP configuration for approval.		X
10. Configure and maintain IPAM tool.	X	
11. Maintain an accurate record of network numbers and physical networks to which they are assigned.	X	
12. Produce reports showing network range allocations and device name and address assignments as requested by the County.	X	

5.16. New Site Installation Services

5.16.1 Overview

This section pertains to the New Site Installation Services Framework Component within the Network Services Framework. The New Site Installation Services Framework Component applies to the Plan and Build tasks needed for a new, networked County Site.

New Site Installation is composed of two distinct sets of tasks:

1. New Site Install Fixed Component is determined by Site Type. The activities within this component allows the Site to connect to the County network. This Fixed Component is required for the establishment of any New Site and will include, but not limited to:

- Establishing design standards and design for the new Site
- Ordering and coordinate all circuits necessary for the new Site
- Conducting all planning and engineering required to ensure site functionality
- Installing network Hardware and Software
- Provisioning of the New Site

2. New Site Install Variable Component, as set forth in Appendix 1 to Exhibit 16.1-1, is determined by infrastructure of the site and Site Type. Included in the Variable Component are activities that include, but are not limited to:

- Setting up of MDF/IDF
- Installing intra building cable plant including all wall jacks, labels, patch panels, testing and certification of cable plant
- Project management for the installation of these components

The County may choose to contract directly with Third-Party vendors to perform some or all of the New Site Install Variable Component activities.

Site Types are based on the number of Cable Drops that will be installed at the New Site. A Cable Drop is defined as the copper horizontal cable which reaches from the Intermediate Distribution Frame (IDF) to the wall jack. The table below outlines the Cable Drop thresholds for each different Site Types.

Site Type	Minimum Cable Drops	Maximum Cable Drops
I	1,000	or more
II	501	999
III	250	500
IV	50	249
V	11	49
VI	1	10

5.16.2 High Level Requirements

5.16.2.1 Contractor shall establish and maintain a Fixed Component based on Site Type for New Site Installation.

5.16.2.2 Contractor shall establish and maintain Variable Component (e.g. MDF, IDF, backbone cable, etc.) based on Site Type.

5.16.2.35.16.2.3 If the County elects to procure cabling installation services outside the Agreement: 1. Contractor shall receive certification stating that a full test of all Cable Drops have been performed and that the installation meets the provided standards. 2. Contractor shall perform IMARs on the New Site as of the Turnover Date, as defined in the Standards and Procedures Manual. 3. Contractor shall not be held responsible for any defect in workmanship or materials discovered within six months of the Turnover Date. Correction of such defects by the Contractor shall be performed under a Service Request.

5.16.3 Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with New Site Installation Services.

New Site Installation Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Submit Service Request to initiate New Site Installation indicating Site Type.		X
2. Produce and submit plans for New Site Installation including breakdown of variable components.	X	
3. Review and approve plans and scope of work for New Site Installation.		X
4. Produce and submit procedures for New Site Installation.	X	
5. Review and approve procedures for New Site Installation.		X
Build Roles and Responsibilities	**Contractor**	**County**

New Site Installation Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
6. Design and implement New Site Installation.	X	
7. Implement County approved policies and procedures for New Site Installation.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
8. Support New Site Installation policies and procedures.	X	

5.17. Interactive Voice Services

5.17.1. Overview

This section pertains to the Interactive Voice Services (Interactive Voice Response (IVR) within the Network Services Framework. The Interactive Voice Services Framework Component applies to the Hardware and Software needed to operate the service within the County.

Interactive Voice Services shall be defined as an IVR system which provide one or more of the following capabilities:

- Call Recording
- Call Management Reporting
- Speech Recognition Application
- Computer Screen POP
- Wallboard (Physical/Virtual)
- Data Integration (Data Dip)
- Work Force Optimization
- Outbound/Predictive Dialer
- Agent Softphone
- Speech Enabled Customer Surveys

5.17.2. High Level Requirements

5.17.2.1. Contractor shall develop plan, implement and integrate a consolidation, modernization and improvement in overall reliability and failover for all County IVS Services.

5.17.2.2. Contractor shall recommend a plan for County approval, and execute the approved plan for changes to continuously reduce County usage costs for Interactive Voice Services.

5.17.2.3. Contractor shall deploy and maintain Interactive Voice Services to meet service requirements.

5.17.2.4. Contractor shall develop and maintain three (3) categories of IVS: Small, Medium and Large.

5.17.2.5. Contractor shall continuously provide and update documentation that details operation and use of Interactive Voice services and post them on the Service Portal.

5.17.2.6. Contractor shall recommend, for County approval, technology and architectural standards on a yearly basis for all Interactive Voice Services.

5.17.2.7. Contractor shall provide the following changes to Interactive Voice Services systems:

- Additions, changes or deletions to existing call flow/menu prompts
- Additions, changes or deletions to existing routing or transfer points
- Professional voice recording of changes
- Implementation of existing/available/already purchased licenses

5.17.2.8. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Voice Services.

5.17.3. Environment

The following further describes Interactive Voice Services refresh and the three categories to be provided that shall include technical design, licensing, hardware/software maintenance and support and initial user training.

5.17.3.1. Technology Refresh

Contractor shall refresh Interactive Voice Services Hardware and Software on a 5-year refresh schedule unless otherwise agreed by the County in

writing, and at a County-approved deployment schedule that minimizes disruption and reduces risk.

5.17.3.2.Small IVS

- Automated Call Distribution (ACD)
  - Distributes calls to customer facing agents
  - Supports the total contact center agent population at all County network locations
  - Includes trunking infrastructure to support the routing of calls
  - Can be used as a stand-alone component or in conjunction with an Auto Attendant
- Auto Attendant (AA)
  - Supports Touch-tone input to route calls across the County voice network
  - Includes the professional recordings both English and Spanish menus and prompts
  - Includes trunking infrastructure to support the routing of calls
  - Can be used as a stand-alone component or in conjunction with an ACD
- Call Management System (CMS)
  - Provides reports of contact center agent metrics such as abandoned calls, average talk time, etc.
  - Used in conjunction with an ACD to manage contact center performance
  - CMS is the additive feature which initiates the Small IVS RU category vs. the right-to-use ACD and/or AA capability associated with the Voice RUs

5.17.3.3.Medium IVS

- Automated Call Recording (ACR)
  - Provides for up to 90 days of customer agent recorded calls for both compliance and quality purposes

- Virtual Wallboards
  - Provides ACD statistics and messages displayed on contact center agent and supervisor desktops
- Agent Softphone
  - Provides IP softphone via a desktop client that will provide County contact center agents full functionality whether they are working at their primary County facility, a remote/alternate County site or at home

5.17.3.4.Large IVS

- Interactive Voice Response (IVR)
  - Platform for custom applications such as outbound predictive dialing, multi-language support, voice recognition and County data integration
- Computer-Telephony Interface
  - Customizable interface between IVR and Desktop components to provide database information to a contact center agent when a constituent call
- Short Message Service (SMS)
  - Provides up to 200,000 outbound text messages to specifically defined County client lists
  - Requires the manual upload of a County file of customer contact information to the hosted platform
- Work Force Management
  - Centralized platform of work force scheduling, forecasting and adherence of contact center agents
  - Provides long term strategic forecasting of agent resource requirements based on historical data
  - Integrated with CMS for agent call statistics
- Physical Wallboards
  - Provides ACD statistics and messages displayed on physical monitors in County call centers
  - Includes the controller infrastructure and supporting software to County provided monitors

5.17.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with IVS Services.

IVS Service Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit plans for IVS Services.	X	
2. Review and approve plans for IVS Services.		X
3. Produce and submit procedures for IVS Services.	X	
4. Review and approve procedures for IVS Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
5. Design and implement IVS Services.	X	
6. Implement County approved policies and procedures for IVS Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Support IVS Services policies and procedures.	X	

5.18. Mobility Services

5.18.1. Overview

This section pertains to the Mobility Services Framework Component within the Network Services Framework.

Services provided by this Framework Component will include some or all of the following:

- Unlimited voice and data carrier plans
- Standardized mobile devices
- FirstNet mobile network access
- Free calling to Mexico and Canada
- Mobile device tethering
- Mobile WiFi Hotspot

5.18.2. High Level Requirements

5.18.2.1. Contractor shall provide voice, data and text mobile plans.

5.18.2.2. Contractor shall recommend standard mobile devices and hotspot routers for County review and approval using the established EA process.

5.18.2.3. Contractor shall offer for purchase, via the OIC, standard mobile devices and hotspot routers. The specifications of these devices shall be listed in the Standards and Procedures Manual.

5.18.2.4. Contractor shall provide the County with access to the FirstNet nationwide, high-speed, broadband network dedicated to public safety.

5.18.3. Environment

The following further describe, and scope Mobility Services elements supported by Contractor and with which Contractor shall comply.

5.18.3.1. Hardware and Software

Contractor shall provide all, voice and data plans, mobile devices, and mobile hotspots.

5.18.3.2. Technology Upgrade and Refresh

Mobile devices supported within Mobility Services are eligible for replacement or upgrade through purchases from the OIC (leveraging subsidized offers) at the end of its two-year support cycle.

5.18.4. Roles and Responsibilities

Mobility Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Provide mobile device recommendations and specifications.	X	
2. Review and approve mobile device recommendations and specifications.		X
3. Provide mobile plan features and capabilities.	X	
4. Develop IMAR and Break Fix Helpdesk scripts for Mobility Services.	X	
5. Develop OIC plans for approved mobile device.	X	

Mobility Services Roles and Responsibilities		
6. Provide OIC information for mobile device and RU ordering.	X	
7. Review and approve plans for mobile carrier plans and mobile device processes.		X
Build Roles and Responsibilities	**Contractor**	**County**
8. Build Help Desk Scripts for both mobile devices and carrier plans.	X	
9. Implement Help Desk scripts for mobile carrier and device issues	X	
10. Deploy OIC offerings for mobile devices and carrier plan.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
11. Provision mobile carrier plans as ordered by the County.	X	
12. Ship mobile devices to County end users as ordered thru the OIC.	X	
13. Provide IMAR and Break Fix Helpdesk services for Mobility Services.	X	

6. DATA CENTER SERVICES

6.1. Overview

Data Center Services include the Hardware, Software and services to support County business applications and data in a secure, consolidated, physical Tier 3 or Tier 4 data center. This includes public cloud environments and services if approved by the County. The data center must be capable of providing hybrid services to County approved cloud based applications and services, be a highly virtualized environment with respect to network, storage and servers and must maintain its own installed and secure Internet connection.

Data Center Services Framework consists of the Plan, Build and Operate services that include the Hardware, Software, Locations and services associated with centralized, shared computing environment.

Data Center Services Framework is composed of the following Framework Components:

- Security Services
- Mainframe Services
- Application Infrastructure Services
- Infrastructure Services
- Development and Test Services
- E-Mail Services
- Unified Communications Infrastructure Services
- Storage Services
- Backup and Recovery Services
- Managed Print Services
- Public Key Infrastructure (PKI) Services

6.2. High Level Requirements

6.2.1. Contractor shall recommend, for County approval, qualified Data Center Service Manager as Contractor Key Personnel to manage Data Center Services.

6.2.2. Contractor shall meet the County needs for highly available, reliable, scalable, up-to-date, agile and secure Data Center Services

6.2.3. Contractor shall maintain a stable, reliable infrastructure to support business applications and services throughout the County.

6.2.4. Contractor shall provide a reliable, scalable, responsive, technically current and secure data network within Data Center Services.

6.2.5. Contractor shall provide redundant, secure, Internet connections for County data center operations within the physical data centers.

6.2.6. Contractor shall maintain Data Center Services network so there is not a single point failure thereby assuring County business continues to operate during any unplanned event.

6.2.7. Contractor shall provide architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Data Center Services.

6.2.8. Contractor shall continuously investigate emerging technology and services that improve the overall data center efficiencies, lowers overall data center costs and improves End-User performance and security when interacting with data center services.

6.2.9. Contractor shall continuously incorporate technology security improvements for business requirements without compromising the security, integrity, and performance of the County enterprise and information resources.

6.2.10. Contractor shall continuously refresh and consolidate Data Center Services Hardware and Software to ensure operability supportability and cost optimization.

6.2.11. Contractor shall continuously identify and correct, with County approval, any single point failures found within Data Center Services.

6.2.12. Contractor shall perform centralized management and performance monitoring of Data Center Services.

6.2.13. Contractor shall continuously ensure that all Data Center Services Hardware and Software are operating at optimal and maximum performance.

6.2.14. Contractor shall report performance, capacity results monthly on all Data Center Services.

6.2.15. Contractor shall deliver and review with County on an annual basis all standards, plans, support tools, version changes, infrastructure changes, refresh, or any matter related to the Data Center and used in the Data Center. This may include future efforts by the Contractor to change services within the Data Center that may or may not affect the County.

6.2.16. Contractor shall continuously review, implement and manage software licensing for Data Center Services assuring best value, non-duplicative installs, inventory, consolidated and documented.

6.2.17. Contractor shall maintain a timeline/roadmap of all Data Center Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

6.2.18. With County approval, Contractor shall provide, integrate, and support public cloud-based environments and services. Specific functional requirements for these services are defined in the relevant Service Framework requirements below based on the solution design for Infrastructure as a Service (Iaas) and/or Platform as a Service (PaaS), e.g., servers, storage, firewalls, databases.

6.3. Environment

6.3.1. Scope of Environment

Data Center Services shall provide Services to all County Locations for all County business functions and external users of County services.

6.3.2. Hardware and Software

Contractor shall provide all Hardware, Software, licenses, tools needed in the delivery of Data Center Services. Contractor shall own, license, provision, install, manage, maintain, and support such Assets.

6.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Data Center Services.

Data Center Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for Data Center Services Framework solutions that best meet County business needs.	X	
2. Review and approve recommendations for Data Center Services Framework solutions that best meet County business needs.		X
3. Produce and submit operational planning for Data Center Services Framework capacity and performance purposes.	X	
4. Review and approve operational planning for Data Center Services Framework capacity and performance purposes.		X
5. Produce and submit recommendations for establishing standards, defining architecture and new project initiatives in the Data Center Services Framework.	X	
6. Review and approve recommendations for establishing standards, defining architecture and new project initiatives in the Data Center Services Framework.		X
7. Recommend architectural components and designs to support the approved data center digitization initiatives.	X	
8. Review and approve architectural components and designs to support the approved data center digitization.		X
9. Develop data center architectural transformation roadmaps in support of any digitization activities.	X	
10. Review and approve data center architectural transformation roadmaps in support of any digitization activities.		X
11. Customize technology architecture taxonomy to meet the evolving business needs of the County.	X	
12. Review and approve the technology architecture taxonomy to meet the evolving business needs of the County.		X
13. Produce and submit recommended Data Center Services administration policies and procedures.	X	
14. Review and approve Data Center Services administration policies and procedures.		X

Data Center Services Roles and Responsibilities		
15. Produce and submit operational documentation on system functions, change management, and Incident management processes.	X	
16. Review and approve operational documentation on system functions, change management, and Incident management processes.		X
17. Produce and submit recommendations on hardware standards for Data Center Services Assets.	X	
18. Review and approve hardware standards for Data Center Services Assets.		X
19. Produce and submit recommendation on software standards for Data Center Services Assets.	X	
20. Review and approve software standards for Data Center Services Assets.		X
21. Produce and submit recommendation for upgrades to Data Center Services Assets as needed to meet business needs.	X	
22. Review and approve upgrades to Data Center Services Assets as needed to meet business needs.		X
23. Produce and submit plans for security updates to Data Center Services Assets.	X	
24. Review and approve plans for security updates to Data Center Services Assets.		X
25. Produce and submit yearly Data Center Services asset consolidation strategy.	X	
26. Review and approve yearly Data Center Services asset consolidation strategy.		X
27. Comply with County policies, standards and regulations applicable to County including information systems, personnel, physical and technical security.	X	
28. Develop a single, consolidated data center for production operations.	X	
29. Develop a technology refresh, redundant systems and improved application architecture design.	X	
30. Collaborate with County to provide technology assistance and support with planning and standard setting activities.	X	

Data Center Services Roles and Responsibilities		
31. Develop a secure flexible Services model when and where appropriate so that the County shall have the flexibility to quickly grow or reduce consumption, including (but not limited to): • Mainframe processing • Storage Area Network (SAN) and Network Attached Storage (NAS) • Centralized backups • Centralized monitoring	X	
32. Create all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to County.	X	
Build Roles and Responsibilities	**Contractor**	**County**
33. Provide all design and engineering required to support Data Center Services Framework.	X	
34. Produce and submit to County all design and engineering documentation.	X	
35. Review and approve all design and engineering documentation.		X
36. Provide all test Services required to support Data Center Services Framework.	X	
37. Produce and submit to County all test documentation.	X	
38. Review and approve all test documentation.		X
39. Implement the approved architectural roadmaps and technology architecture taxonomy across the data centers.	X	
40. Manage deployment efforts using formal project management tools, methodologies and standards (e.g., ITIL change and configuration management practices).	X	
41. Deploy code and content using automated tools which include publishing, promoting, and rolling back code and content.	X	
42. Conduct deployment reviews and provide results to County.	X	
43. Review and approve results of deployment reviews.		X
44. Install security patches and security products.	X	
Operate Roles and Responsibilities	**Contractor**	**County**

Data Center Services Roles and Responsibilities		
45. Publish all Data Center Services asset standards on the Service Portal.	X	
46. Provide support, including breakfix, for all Data Center Services Assets.	X	
47. Perform maintenance activities during nonpeak hours (shall be determined in coordination with the County).	X	
48. Provide the County with a system software upgrade list as it becomes available from software suppliers in the form of a technology roadmap that has a timeline based on version life cycle.	X	
49. Measure, monitor, and adjust data center system and network parameters to make certain the required level of performance is maintained.	X	
50. Analyze performance management information of current and expected capacity to make recommendations for server upgrades, load balancing, and functional splitting. Evaluate trend data and factor it into the overall system requirements.	X	
51. Manage event and workload processes across all platforms.	X	
52. Provide technical support for all hardware/equipment of the Data Center computing infrastructure.	X	
53. Support Data Center infrastructure System software (e.g., operating systems, utilities, databases, Middleware).	X	
54. Provide and support Data Center Networks (e.g., LAN, WAN connection) and related operations (e.g., procure, design, build, systems monitoring, Incident diagnostics, troubleshooting, Resolution and escalation, security management, and capacity planning/analysis) as required to meet County computing requirements.	X	
55. Provide and support Data Center-related environmental elements (e.g., HVAC, dual redundant UPS, power, cable plant, fire detection and suppression systems, temperature and humidity controls, and controlled physical access with 24/7/365 manned security).	X	
56. Support applications test-to-production migration activities infrastructure.	X	

Data Center Services Roles and Responsibilities		
57. Implement and coordinate all changes to the Data Center infrastructure including those that affect the Service Levels of any other Framework and Third-Parties.	X	
58. Maintain and provide all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to County.	X	
59. Provide threat scanning services on files uploaded by public to County servers. Monitor and reports threats.	X	

6.5. Security Services

6.5.1. Overview

The Security Services Framework Component of the Data Center Services Framework includes the Hardware, Software, and services needed to maintain overall managed security for the Services. Security Services provided by this Framework Component include, but are not limited to, the following:

- Monitored or managed firewalls or intrusion prevention systems (IPSs)
- Monitored or managed intrusion detection systems (IDSs)
- Monitored or managed multifunction firewalls, or unified threat management (UTM) technology
- Managed or monitored security gateways for messaging or Web traffic
- Security analysis and reporting of events collected from infrastructure logs
- Reporting associated with monitored/managed devices and incident response
- Managed vulnerability scanning of networks, servers, databases or applications
- Distributed denial of service (DDoS) protection
- Monitoring or management of customer-deployed security information and event management (SIEM) technologies
- Monitoring and/or management of advanced threat defense technologies, or the provision of those capabilities as a service
- Transformational activities to improve the overall security, increase performance and lower costs
- Security architecture services

6.5.2. High Level Requirements

6.5.2.1. Contractor shall control physical access to the Data Center.

6.5.2.2. Contractor shall establish secure zones, with County approval, in the Data Center network.

6.5.2.3. Contractor shall lock down all servers (physical or virtual) and storage within the Data Center.

6.5.2.4. Contractor shall scan all applications, prior to release into production, for vulnerabilities.

6.5.2.5. Contractor shall increase visibility into all data communications and data flows between applications within the Data Center and cloud-based applications.

6.5.2.6. Contractor shall ensure necessary throughput for perimeter protection and internal security methods that are fast enough to deeply scan and remediate threats at wire speed.

6.5.2.7. Contractor shall ensure that Data Center architecture is built with a security first mindset.

6.5.2.8. Contractor shall implement a "single pane of glass" approach to management and monitoring Security Services.

6.5.2.9. Contractor shall ensure all Hardware and Software used for the delivery of Security Services is virtual environment aware.

6.5.2.10. Contractor shall provide management, refresh, support, reporting and logging of all firewalls used in the delivery of the Services.

6.5.2.11. Contractor shall provide information event logging, analysis, reporting and management of all Hardware and Software used to provide Security Services.

6.5.2.12. Contractor shall provide log management on cloud-based applications used by the County.

6.5.2.13. Contractor shall provide intrusion detection and prevention systems within the Data Centers.

6.5.2.14. Contractor shall provide unified threat management.

6.5.2.15. Contractor shall update all Hardware and Software used for Security Services to the latest patch, service packs, or other updates promptly to ensure operational integrity.

6.5.2.16. Contractor shall refresh all Hardware and Software used for Security Services on a 4-year cycle unless otherwise approved by the County.

6.5.2.17. Contractor shall ensure that all Hardware and Software used in the delivery of Security Services is identified whether it is leveraged across multiple accounts or dedicated to the County.

6.5.2.18. Contractor shall maintain all Hardware used in the delivery of Security Services to maximize performance with high-speed network operations.

6.5.3. Environment

6.5.3.1. Hardware and Software

Contractor shall provide all Hardware, Software, tools, knowledge databases, logging and analysis and used in the delivery of Security Services. Contractor shall own, provision, install, manage, maintain, and supported such Assets.

6.5.3.2. Facilities

All Data Center based applications, data, services and cloud-based applications managed by the Contractor for Security Services.

6.5.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Security Services.

Security Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit a Security architecture for Data Center Services.	X	
2. Review and approve Security architecture for Data Center Services.		X
3. Develop and submit plans for pre-release of Portfolio Applications or any other data center changes scan and vulnerability analysis.	X	
4. Review and approve plan for scan and vulnerability analysis.		X
5. Develop and submit annual operational procedures for data center Security Services.	X	
6. Produce and submit methodology and performance tools to assess and remediate data center security Incidents.	X	
7. Review and approve methodology and performance tools to assess and remediate data center security Incidents.		X
8. Develop and submit design and plans for SIEM tool.	X	
9. Review and approve design and plans for SIEM tool.		X
10. Produce and submit monitoring and managing of all Security Services Hardware and Software.	X	
11. Review and approve monitoring and managing of all Security Services Hardware and Software.		X
12. Produce and submit annual refresh plans for Security Services.	X	
13. Review and approve submit annual refresh plans for Security Services.		
14. Produce and submit security plan for cloud-based services used in hybrid mode.	X	
15. Review and approve security plan for cloud-based services used in hybrid mode.		X
16. Produce and submit lock-down scripts for Data Center Services.	X	

Security Services Roles and Responsibilities		
17. Review and approve lock-down scripts for Data Center Services.		X
18. Develop process to continuously post all documentation developed and maintained in Security Services to the Service Portal.	X	
Build Roles and Responsibilities	**Contractor**	**County**
19. Implement and maintain security architecture in Data Center Services.	X	
20. Develop monthly reports on SIEM and other Incidents affecting security in Data Center Services.	X	
21. Implement single pane management console for Security Services.	X	
22. Perform refresh according to the approved annual refresh plans for Security Services.	X	
23. Implement and monitor security plan for cloud-based services used in hybrid mode.	X	
24. Implement lock-down scripts for Data Center Services.	X	
25. Design, test and implement all policies needed to provide Security Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
26. Review and analyze SIEM activity and report findings monthly.	X	
27. Recommend changes based on operational experiences to the security architecture supporting Security Services.	X	
28. Support all Data Center Services Incidents.	X	
29. Support all Severity 1 Incidents.	X	
30. Continuous review data center for vulnerabilities and recommend corrections promptly.	X	
31. Update Security Services with patches or other updates promptly to assure operational integrity.	X	

6.6. Mainframe Services

6.6.1. Overview

The Mainframe Service Framework Component of Data Center Services applies to the services and support for the Mainframe and AS/400.

6.6.2. High Level Requirements

6.6.2.1. Contractor shall develop, for County approval, and execute plans to retire the Mainframe from the Services.

6.6.2.2. Contractor shall develop, for County approval, and execute plans to retire the A/S400 from the Services.

6.6.2.3. Contractor shall measure Mainframe usage in CPU hours and must correlate CPU hours directly to End-User processing for specific application.

6.6.3. Environment

6.6.3.1. Hardware and Software

6.6.3.1.1. Contractor shall provide all Hardware, Software and utilities to support Mainframe Services.

6.6.3.1.2. All licensing shall be the responsibility of the Contractor for all Hardware and Software used to provide Mainframe Services.

6.6.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities specific to Mainframe Services.

Mainframe Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit plans to retire the Mainframe and AS/400 upon Service Request.	X	
2. Review and approve plans to retire the Mainframe and AS/400.		X
3. Produce and submit recommendations for standards on production jobs and Job Control Language (JCL).	X	
4. Review and approve recommendations for standards on production jobs and Job Control Language (JCL).		X
Operate Roles and Responsibilities	**Contractor**	**County**
5. Continue to support mainframe and AS/400 operationally.	X	

6.7. Application Infrastructure Services

6.7.1. Overview

This section pertains to the Application Infrastructure Services Framework Component within the Data Center Framework. The Application Infrastructure Services Framework Component applies to all Hardware and Software needed to maintain and support County Portfolio Applications.

The Application infrastructure is a platform of integrated technologies that can manage multiple hosted applications. The Application infrastructure is comprised of application servers, web servers, and database servers and is a core applications architecture component. The Application infrastructure will deliver high performance application services to End-Users, Third-Parties and constituents of the Services. Some of the key functionality of the Application infrastructure includes, but is not limited to, transaction management, clustering, application-to-application messaging, system management, advanced application development tools, proprietary access, and interoperability with legacy technologies. Application infrastructure provides a powerful platform to support and extend a broad range of County Portfolio Applications.

Building a multi-tier architecture is foundational for the Application infrastructure. Example for multi-tier architecture is as follows:

- A first-tier, front-end, browser-based presentation layer
- A middle-tier business logic application or set of applications
- A third-tier, back-end, database and transaction server

Application Infrastructure Services Framework Component include, but are not limited to, Server refresh, operating system update and support, management of server resources, monitor and analyze network performance, overall application performance, server performance and capacity tuning and analysis.

6.7.2. High Level Requirements

6.7.2.1. Contractor shall ensure that County Portfolio Applications are hosted exclusively in the Application Infrastructure Services.

6.7.2.2. Contractor shall provide continuous operating system updates, patches and security hot fixes for Application infrastructure.

6.7.2.3. Contractor shall deploy County preferred and standard virtual servers, virtual storage and virtual network.

6.7.2.4. Contractor shall gain approval by the County for any exception to the virtual first standards.

6.7.2.5. Contractor shall provide annual refresh plans for all virtual services.

6.7.2.6. Contractor shall provide annual server consolidation recommendations.

6.7.2.7. Contractor shall continuously monitor and correct performance Incidents or system degradation for all application servers.

6.7.2.8. Contractor shall maintain Application infrastructure storage on centralized, shared storage environment.

6.7.2.9. Contractor shall provide server hardening across Application infrastructure.

6.7.2.10. Contractor shall implement a data backup strategy to meet County Applications' requirements.

6.7.2.11. Contractor shall support and assist in Third-Party application installation and configuration.

6.7.2.12. Contractor shall improve overall architecture of the Application infrastructure with consideration of cloud and increased virtualization techniques.

6.7.2.13. Contractor shall continuously improve demand levels across the Application infrastructure.

6.7.2.14. Contractor shall continuously improve and reduce costs with integrated tools that provide better security and control of the Application infrastructure.

6.7.2.15. Contractor shall deploy and use standard operating systems on all Hardware used to provide Application Infrastructure Services.

6.7.2.16. Contractor shall continuously improve speed of delivery for new Applications and Services in Application infrastructure.

6.7.2.17. Contractor shall continuously deliver to business objectives while reducing overall Application infrastructure costs across all environments.

6.7.2.18. Contractor shall provide centralized support and tools for Application servers located outside the data center.

6.7.2.19. Contractor shall maintain a timeline/roadmap of all Application Infrastructure Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

6.7.2.20. Contractor shall maintain and be responsible for all components needed to provide Application Infrastructure Services.

6.7.2.21. Contractor shall maintain Application Infrastructure Services so there is not a single point failure thereby assuring County business applications continue to operate during any unplanned event.

6.7.2.22. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Application Infrastructure Services.

6.7.2.23. Contractor shall continuously investigate emerging technologies and services that improve the overall Application infrastructure

efficiencies, lowers overall costs and improves business application performance and security.

6.7.2.24. Contractor shall provide Low Code Application Platform Services.

6.7.3. Environment

6.7.3.1. Hardware and Software

6.7.3.1.1. Contractor shall provide all Hardware, Software and utilities to support Application Infrastructure Services.

6.7.3.1.2. All licensing shall be the responsibility of the Contractor for all Hardware and Software used to provide Application Infrastructure Services.

6.7.3.2. Wintel Application Infrastructure Services

WINTEL Application Infrastructure Services are the Microsoft Server operating system based virtual and physical servers supporting Application Infrastructure Services.

6.7.3.2.1. Contractor shall recommend, for County approval, annual standards for virtual and physical hardware.

6.7.3.2.2. Contractor shall deploy annual, County approved, virtual and physical hardware standards.

6.7.3.2.3. Contractor shall publish all County approved standards in the Standards and Procedures Manual on the Service Portal.

6.7.3.2.4. Contractor shall develop hardware standards shall be set for three classes of physical server types: Small, Medium, Large, and X-Large.

6.7.3.2.5. Contractor shall maintain, with sufficient capacity, a server farm to host all virtual servers.

6.7.3.2.6. Contractor shall develop, install and maintain all storage for Application Infrastructure Services using centralized Storage Area Network (SAN).

6.7.3.2.7. Contractor shall recommend, for County approval, annual standards for Windows Operating Systems for virtual and physical servers.

6.7.3.2.8. Contractor shall maintain operating system currency on all Application Infrastructure Services.

6.7.3.2.9. Contractor shall refresh all physical servers at a rate of 25% per year. No physical server shall be in service longer than 4 years without County written approval.

6.7.3.2.10. Contractor shall perform refresh activities using a straight-line methodology throughout the Contract Year.

6.7.3.2.11. Contractor shall maintain and update, for County review, timeline/roadmap of all Hardware and Software product life cycles for Application Infrastructure Services.

6.7.3.2.12. Contractor shall responsible for all activities related to virtual or physical server refresh, including business application reinstall and configuration.

6.7.3.3. UNIX Application Infrastructure Services

UNIX Application Infrastructure Services are the UNIX operating system based virtual and physical servers supporting Application Infrastructure Services.

6.7.3.3.1. Contractor shall recommend, for County approval, annual standards for virtual and physical hardware.

6.7.3.3.2. Contractor shall deploy annual, County approved, virtual and physical hardware standards.

6.7.3.3.3. Contractor shall publish all County approved standards in the Standards and Procedures Manual on the Service Portal.

6.7.3.3.4. Contractor shall develop hardware standards shall be set for three classes of physical server types: Small, Medium, Large and X-Large.

6.7.3.3.5. Contractor shall develop, deliver, for County approval, and implement an infrastructure to support virtualization of UNIX servers.

6.7.3.3.6. Contractor shall maintain, with sufficient capacity, a server farm to host all UNIX based virtual servers.

6.7.3.3.7. Contractor shall develop, install and maintain all storage for UNIX Application Infrastructure Services using centralized Storage Area Network (SAN).

6.7.3.3.8. Contractor shall recommend, for County approval, annual standards for UNIX Operating Systems for virtual and physical servers.

6.7.3.3.9. Contractor shall maintain, potentially, different sources for UNIX operating systems.

6.7.3.3.10. Contractor shall maintain operating system currency on all UNIX Application Infrastructure Services.

6.7.3.3.11. Contractor shall refresh all physical servers at a rate of 20% per year. No physical server shall be in service longer than 5 years without County written approval.

6.7.3.3.12. Contractor shall perform refresh activities using a straight line methodology throughout the Contract Year.

6.7.3.3.13. Contractor shall maintain and update, for County review, timeline/roadmap of all Hardware and Software product life cycles for Application Infrastructure Services.

6.7.3.3.14. Contractor shall responsible for all activities related to virtual or physical server refresh, including business application reinstall and configuration.

6.7.3.4. Virtual Application Infrastructure Services

Virtual Application Infrastructure Services are the requirements for supporting Windows Application Infrastructure Services and UNIX Application Infrastructure Services.

A Virtual Guest Server is a logical instance of an operating system and applications environment based on the use of virtualization software on a physical host server (Virtual Host). Virtualization software permits the virtualization of a computing environment to support multiple virtual environments.

6.7.3.4.1. Contractor shall recommend, for County approval, annual standards for Virtual Application Infrastructure to support

Windows Application Infrastructure Services and UNIX Application Infrastructure Services.

6.7.3.4.2. Contractor shall deploy annual, County approved, Virtual Application Infrastructure standards.

6.7.3.4.3. Contractor shall determine the number of virtual guest per virtual host server to ensure maximum efficiency and zero service impact due to performance.

6.7.3.4.4. Contractor shall configure and deploy virtual guests to the same standards, or better to physical servers.

6.7.3.4.5. Contractor shall refresh virtual guest servers based on current operating system standards.

6.7.3.4.6. Contractor shall develop and deliver self-service and policy based infrastructure provisioning to the Virtual Application Infrastructure.

6.7.3.4.7. Contractor shall extend the Virtual Application Infrastructure to include software-defined storage platform (Hyper-Converged Infrastructure) integration as standard methodology.

6.7.3.4.8. Contractor shall extend the Virtual Application Infrastructure to integrate and operate in a heterogeneous or hybrid cloud environments.

6.7.3.4.9. Contractor shall design, deliver (for County approval) and implement software-defined storage that can scale for capacity and performance simultaneous as part of virtual guest provisioning.

6.7.3.4.10. Contractor shall design, deliver and implement high availability, fault tolerance and other similar techniques to minimize or eliminate downtime in the Virtual Application Infrastructure.

6.7.3.4.11. Contractor shall deploy tools to ensure all County Portfolio Applications are virtualized and operating in the Virtual Application Infrastructure as standard practice.

6.7.3.4.12. Contractor shall implement management for the Virtual Application Infrastructure that allows the creation, sharing, deployment and migration of virtual guest servers.

6.7.3.4.13. Contractor shall develop, deliver (for County approval), and implement a centralized content library for virtual templates, virtual appliances, ISO images, and scripts.

6.7.3.4.14. Contractor shall develop and implement cloud management platform for purpose-built hybrid cloud applications.

6.7.3.4.15. Contractor shall develop, deliver (for County approval) and implement capacity and performance tools specifically designed for the Virtual Application Infrastructure environment.

6.7.3.4.16. Contractor shall develop the Virtual Application Infrastructure on Industry standard server virtualization platform.

6.7.3.4.17. Contractor shall build and manage virtualization to optimize infrastructure, automate service delivery and provide high availability to virtual guest servers.

6.7.3.4.18. Contractor shall design, deliver, for County approval and implement the virtual farm required to operate the Application Infrastructure Services.

6.7.3.5. Oracle Exadata Services

6.7.3.5.1. Oracle Exadata Services are the compute and storage system for running Oracle Database software supporting Application Infrastructure Services.

6.7.3.5.2. Contractor shall recommend, for County approval, annual standards for hardware.

6.7.3.5.3. Contractor shall deploy annual, County approved, physical hardware standards.

6.7.3.5.4. Contractor shall publish all County approved standards in the Standards and Procedures Manual on the Service Portal.

6.7.3.5.5. Contractor shall develop hardware standards for Eighth Rack server.

6.7.3.5.6. Contractor shall refresh all Oracle Exadata based Application Servers every 5 years. No physical server shall be in service longer than 5 years without County written approval.

6.7.3.5.7. Contractor shall perform refresh activities using a straight-line methodology throughout the Contract Year.

6.7.3.5.8. Contractor shall maintain and update, for County review, timeline/roadmap of all Hardware and Software product life cycles for Oracle Exadata Services.

6.7.3.5.9. Contractor shall responsible for all activities related to Oracle Exadata based Application servers refresh, including business application reinstall and configuration, except for County-approved remediation of application software.

6.7.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities specific to Application Infrastructure Services.

Application Infrastructure Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for hardware standards of Application Infrastructure Services Assets on a yearly basis.	X	
2. Review and approve hardware standards for Application Infrastructure Services Assets.		X
3. Produce and submit recommendations for operating system standards for Application Infrastructure Services Assets on a yearly basis.	X	
4. Review and approve operating system standards for Application Infrastructure Services Assets.		X
5. Produce and submit Application Infrastructure Services refresh plan on a yearly basis.	X	
6. Review and approve Application Infrastructure Services refresh plan.		X
7. Produce and submit Application Infrastructure Services storage migration and consolidation plan on a yearly basis.	X	

Application Infrastructure Services Roles and Responsibilities		
8. Review and approve Application Infrastructure Services storage migration and consolidation plan.		X
9. Produce and submit backup/recovery policies and procedures.	X	
10. Review and approve backup/recovery policies and procedures.		X
11. Produce and submit recommendations for Application Infrastructure placement into County Locations.	X	
12. Review and approve recommendations for Application Infrastructure placement into County Locations.		X
13. Produce and submit recommendations for Application Infrastructure Services consolidation plan on a yearly basis.	X	
14. Review and approve Application Infrastructure Services consolidation plan.		X
15. Produce and submit Application Infrastructure Services Assets plans for updates or patches as needed for reliable operations and to maintain security.	X	
16. Review and approve Application Infrastructure Assets Services plans for updates or patches as needed for reliable operations and to maintain security.		X
17. Produce and submit recommendations for monitoring and exceptional conditions procedures.	X	
18. Review and approve monitoring and exceptional conditions procedures.		X
19. Produce and submit recommendations for job scheduling requirements, interdependencies, County contacts, and rerun requirements for all production jobs.	X	
20. Review and approve job scheduling requirements, interdependencies, County contacts, and rerun requirements for all production jobs.		X
21. Recommend replacement or upgrade of County utility software programs with commercially available software to support processing operations.	X	
22. Develop Low Code Application Platform solution design document including but not limited to architecture, functions, data models, design features, configuration, performance requirements (e.g., security, extensibility, maintainability, scalability, availability, and reliability).	X	

Application Infrastructure Services Roles and Responsibilities		
23. Review and approve a Low Code Application Platform solution design document including but not limited to architecture, functions, data models, design features, configuration, performance requirements (e.g., security, extensibility, maintainability, scalability, availability, and reliability).		X
24. Develop standards and governance processes for the Low Code Application environment, including but not limited to release management, code reviews, application specification documentation, and code promotion, under the Low Code Center of Excellence.	X	
25. Review and approve standards and governance processes for the Low Code Application environment, including but not limited to release management, code reviews, application specification documentation, and code promotion, under the Low Code Center of Excellence.		X
Build Roles and Responsibilities	**Contractor**	**County**
26. Provide all design and engineering required to deploy, refresh and support Application Infrastructure Services Assets.	X	
27. Design, test and implement hardware standards for Application Infrastructure Services Assets.	X	
28. Design, test and deploy operating system standards for Application Infrastructure Services Assets.	X	
29. Deploy, manage, communicate and report on activities related to Application Infrastructure Services refresh.	X	
30. Review and approve reports on Application Infrastructure Services refresh.		X
31. Design, test and execute Application Infrastructure Services storage migration and consolidation plan.	X	
32. Implement approved backup/recovery policies and procedures.	X	
33. Design, test and deploy approved Application Infrastructure Services consolidation plans.	X	
34. Test and deploy approved updates or patches to Application Infrastructure Services Assets.	X	
35. Implement the Low Code Application Platform based on the approved solution design document.	X	

Application Infrastructure Services Roles and Responsibilities		
36. Update Low Code Application Platform architecture documents as needed (e.g., enhancements).	X	
37. Review and approve updates to Low Code Application Platform architecture documents.		X
Operate Roles and Responsibilities	**Contractor**	**County**
38. Provide support for Application PreProduction and Application Test Servers.	X	
39. Conduct data and Application migration that is necessary due to any Application Infrastructure refresh or breakfix activity.	X	
40. Monitor, operate, maintain and support the Third-Party Applications running on Application servers.	X	
41. Provide automated event monitoring tools that notify Applications Team for immediate response if there is an applicationrelated Incident.	X	
42. Provide support, including breakfix, for all Application Infrastructure Services Assets.	X	
43. Provide support for Application Infrastructure located in County Locations.	X	
44. Provide support for Application Infrastructure Services storage migration and consolidation plan.	X	
45. Perform backups on Application Infrastructure Services Assets as defined.	X	
46. Conduct data and Application migration that is necessary due to any Application Infrastructure refresh or breakfix activity.	X	
47. Support send and receive electronic data transmissions (e.g., EDI, FTP).	X	
48. Perform upgrades, updates, and security patching to Application Infrastructure Service Assets.	X	
49. Monitor, operate, maintain and support OS (Operating Systems) installed on Application Infrastructure.	X	
50. Monitor, operate, maintain and support the Third-Party Applications running on Application Infrastructure.	X	
51. Execute standard operating procedures at scheduled times.	X	

Application Infrastructure Services Roles and Responsibilities		
52. Startup and shutdown County online/interactive systems according to defined schedules or upon approved requests.	X	
53. Coordinate and manage Third-Party hardware and software maintenance to meet County requirements.	X	
54. Ensure that System management and monitoring tools do not impact County operations.	X	
55. Provide automated event monitoring tools that shall notify Applications Team for immediate response if there is an applicationrelated problem.	X	

6.8. Infrastructure Services

6.8.1. Overview

This section pertains to the Infrastructure Services Framework Component within the Data Center Framework. Infrastructure Services refers to the agnostic, Hardware, Software, network resources and services required for the existence, operation and management of the County IT and Telecommunications enterprise. Infrastructure Services shall deliver the Services to County End-Users, Third-Parties, and constituents.

The objective is the continuous improvement in the overall availability of Infrastructure Services to meet the requirements of County business needs. This covers the evaluation, design, implementation, measurement and management of Infrastructure Services availability from a component and an end-to-end perspective including new or modified service management methodologies and tools, as well as technology modifications or upgrades to infrastructure systems and components.

Infrastructure Services provided within this Framework Component include, but are not limited to, server/OS management, server refresh, server/OS tuning, storage and backup management, mainframe services, production operations, performance analysis, capacity analysis and monitoring, and Systems management.

Additional Services within this Framework Component include, but are not limited to, DNS, DHCP, End-User Authentication, directory services, software distribution, print services, FTP and file services, certificate services, proxy services, load balancers, application and network acceleration, network services, task/job scheduling, web and

content filtering and any Contractor internal servers/services needed to fully support the delivery of the Services.

6.8.2. High Level Requirements

6.8.2.1. Contractor shall develop, deliver (for County approval), and implement on an annual basis currency of software across all Infrastructure Services.

6.8.2.2. Contractor shall determine critical business impact to component or system failures in Infrastructure Services.

6.8.2.3. Contractor shall continuously analyze, identify and remediate single point failures in Infrastructure Services.

6.8.2.4. Contractor shall design, deploy and maintain software distribution for Desktop Computing Services and shall integrate and perform software delivery for County mobile devices.

6.8.2.5. Contractor shall continuously monitor and perform maintenance on all load balancers to ensure optimal operational performance.

6.8.2.6. Contractor shall recommend, for County approval, annual standards for Infrastructure Services.

6.8.2.7. Contractor shall deploy and support current standards within Infrastructure Services.

6.8.2.8. Contractor shall provide centralized and standardized system that automates network management of End-User data, security, and distributed resources.

6.8.2.9. Contractor shall automate software distribution including delivering applications, images, and patches to the environment using industry standard tools.

6.8.2.10. Contractor shall perform comprehensive infrastructure testing for all components in an integrated environment for compute, storage, network, database in a physical or virtual environment.

6.8.2.11. Contractor shall ensure County Public Library private network is included in all Infrastructure Services.

6.8.2.12. Contractor shall provide refresh on all Infrastructure Services Hardware and Software on a four (4) year refresh cycle.

6.8.2.13. Contractor shall ensure the Infrastructure Services storage is not comingled with County End-User or Portfolio Application storage.

6.8.2.14. Contractor shall develop Infrastructure Services to include provisions for hybrid-computing and ensure the complete integration of all County cloud based services.

6.8.2.15. Contractor shall ensure that Infrastructure Services are not comingled with County Applications Infrastructure Services.

6.8.2.16. Contractor shall continuously perform capacity planning, utilization analysis for all Infrastructure Services, including the virtual environments.

6.8.2.17. Contractor shall manage and certify OS images used to support Infrastructure Services.

6.8.2.18. Contractor shall ensure Infrastructure Services must be designed and maintained to support County business strategy and County Portfolio Applications.

6.8.2.19. Contractor shall continuously monitor, report and remediate performance Incidents with Infrastructure Services.

6.8.2.20. Contractor shall ensure end-to-end infrastructure, to include mobile, for all County End-User interaction with the Services.

6.8.2.21. Contractor shall ensure Infrastructure Services includes data centers, Locations, colocation facilities, or hosting/cloud services.

6.8.2.22. Contractor shall deploy and maintain application and network acceleration in the delivery of the Services.

6.8.2.23. Contractor shall continuously improve Infrastructure Services performance, speed and decrease overall latency in the delivery of the Services.

6.8.2.24. Contractor shall continuously deliver to meet County business objectives while reducing overall Infrastructure Services costs.

6.8.2.25. Contractor shall provide centralized support and tools for Infrastructure Services located with the data center or outside the data center.

6.8.2.26. Contractor shall maintain a timeline/roadmap of all Infrastructure Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

6.8.2.27. Contractor shall maintain and be responsible for all components needed to provide Infrastructure Services (e.g. load balancers, firewalls, IPS).

6.8.2.28. Contractor shall maintain Infrastructure Services so there is not a single point failure thereby assuring County business applications continue to operate during any unplanned event or outage.

6.8.2.29. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Infrastructure Services.

6.8.2.30. Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security.

6.8.2.31. County may request, on a Service Request, network and application acceleration for a specific County site.

6.8.3. Environment

6.8.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Infrastructure Services.

6.8.3.2. Facilities

Infrastructure Services Hardware or Software placed in County Locations, with County approval, in order to meet the Service Levels and maintain operational efficiencies.

6.8.4. Roles and Responsibilities

The following table identifies the Plan Build and Operate roles and responsibilities associated with Infrastructure Services.

Infrastructure Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations for improvement to Infrastructure Services.	X	
2. Review and approve improvement to Infrastructure Services.		X
3. Produce and submit recommendations for Infrastructure Server placement into Locations.	X	
4. Review and approve recommendations for Infrastructure Server placement into Locations.		X
5. Produce and submit recommendations for hardware standards of Infrastructure Server Services Assets on a yearly basis.	X	
6. Review and approve hardware standards for Infrastructure Server Services Assets.		X

Infrastructure Services Roles and Responsibilities		
7. Produce and submit recommendations for operating system standards for Infrastructure Server Services Assets on a yearly basis.	X	
8. Review and approve operating system standards for Infrastructure Server Services Assets.		X
9. Produce and submit Infrastructure Server Services refresh plan on a yearly basis.	X	
10. Review and approve Infrastructure Server Services refresh plan.		X
11. Produce and submit recommendations for Infrastructure Server Services consolidation plan on a yearly basis.	X	
12. Review and approve Infrastructure Server Services consolidation plan.		X
13. Produce and submit Infrastructure Server Services Assets plans for updates or patches as needed for reliable operations and to maintain security.	X	
14. Review and approve Infrastructure Server Services Assets plans for updates or patches as needed for reliable operations and to maintain security.		X
Build Roles and Responsibilities	**Contractor**	**County**
15. Provide all design and engineering required to deploy, refresh and support Infrastructure Server Services Assets.	X	
16. Design, test and implement approved improvements to Infrastructure Services.	X	
17. Design, test and implement hardware standards for Infrastructure Server Services Assets.	X	
18. Design, test and deploy operating system standards for Infrastructure Server Services Assets.	X	
19. Deploy, manage, communicate and report on activities related to Infrastructure Server Services refresh.	X	
20. Review and approve reports on Infrastructure Server Services refresh.		X
21. Design, test and deploy approved Infrastructure Server Services consolidation plans.	X	
22. Test and deploy approved updates or patches to Infrastructure Server Services Assets.	X	

Infrastructure Services Roles and Responsibilities		
Operate Roles and Responsibilities	**Contractor**	**County**
23. Manage Infrastructure Server Services to meet performance Service Levels.	X	
24. Maintain and support the Public Library public infrastructure web filtering.	X	
25. Manage bandwidth and latency constraints and minimize impacts during automated software deployment.	X	
26. Provide deployment Services using automated tools for remote access/VPN Users.	X	
27. Provide deployment reports to include success and failure statistics of scheduled distributions — such as patches or upgrades.	X	
28. Provide support, including break-fix, for all Infrastructure Server Services Assets.	X	
29. Provide support for Infrastructure Servers located in Locations.	X	
30. Conduct data and Infrastructure migration that is necessary due to any Infrastructure Server Services refresh or break-fix activity.	X	
31. Perform upgrades to Infrastructure Server Services Assets.	X	
32. Monitor, operate, maintain and support OS (Operating Systems) installed on Infrastructure Server Services Assets.	X	
33. Manage Infrastructure Server Services to meet performance Service Levels.	X	
34. Maintain and support the Public Library public infrastructure web filtering.	X	
35. Manage bandwidth and latency constraints and minimize impacts during automated software deployment.	X	
36. Provide deployment services using automated tools for remote access/VPN users.	X	
37. Provide deployment reports to include success and failure statistics of scheduled distributions — such as patches or upgrades.	X	

6.9. Development and Test Services

6.9.1. Overview

This section pertains to the Development and Test Services Framework Component within the Data Center Framework. Development and Test Services are the activities associated with ensuring that all individual technical components configured with or added to the Services work together cohesively to achieve the intended results prior to release to the Production environment.

The activities associated with these Services delivered virtually.

6.9.2. High Level Requirements

6.9.2.1. Contractor shall develop, deliver, for County approval, and implement a private cloud based/hybrid Development and Test Services.

6.9.2.2. Contractor shall build and maintain the Development and Test Services Infrastructure to all standards and in close alignment with the production environment.

6.9.2.3. Contractor shall support in-flight projects, planned projects, maintenance projects and new application releases.

6.9.2.4. Contractor shall manage existing test environments, build new test environments and provide additional capacity on demand via the cloud or other approved County solution.

6.9.2.5. Contractor shall establish the processes and controls that are required to place a County Portfolio Application Development and Test environment in the cloud.

6.9.2.6. Contractor shall develop automation in the management, provision and support of the Development and Test Services Infrastructure to maximize overall system efficiencies.

6.9.2.7. Contractor shall ensure Development and Test Services Infrastructure is integrated into Run Book automation.

6.9.2.8. Contractor shall develop, deliver and maintain cloud orchestration for Development and Test Services Infrastructure.

6.9.2.9. Contractor shall continuously improve overall test environment builds to achieve high efficiencies and accurate test environments.

6.9.2.10. Contractor shall develop the Development and Test Services Infrastructure with a high level of reuse and maximize investments in current tools and technology.

6.9.2.11. Contractor shall continuously develop and implement improvements to overall availability of the Development and Test Services Infrastructure.

6.9.2.12. Contractor shall develop, deliver and implement proper scheduling techniques to maximize the use of the Development and Test Services Infrastructure.

6.9.2.13. Contractor shall develop, deliver and implement processes to ensure the Development and Test Services Infrastructure is not underutilized.

6.9.2.14. Contractor shall ensure sufficient capacity in the Development and Test Services Infrastructure to meet County demand.

6.9.2.15. Contractor shall develop an on-demand Development and Test Services Infrastructure that scales up or down to meet demand.

6.9.2.16. Contractor shall develop, deliver and implement process to cold store virtual and unused workload not currently needed in the Development and Test Services Infrastructure.

6.9.2.17. Contractor shall develop, deliver, for County approval, and implement a fully virtual Development and Test Services Infrastructure.

6.9.2.18. Contractor shall not use any physical servers for the Development and Test Services Infrastructure, without prior County approval.

6.9.2.19. Contractor shall develop, deliver and maintain interfaces to production environment as needed to meet business needs.

6.9.2.20. Contractor shall implement and integrate Identity Access Management Services in the Development and Test Services Infrastructure.

6.9.2.21. Contractor shall replicate production security architecture, to the extent possible, in the Development and Test Services Infrastructure.

6.9.2.22. Contractor shall ensure Development and Test Services Infrastructure duplicates production to the extent possible.

6.9.3. Environment

6.9.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Development and Test Services Infrastructure Services.

6.9.3.2. Licenses

Contractor shall provide all licenses for all cloud based Development and Test Services.

6.9.4. Roles and Responsibilities

The following table identifies the Development and Test Services roles and responsibilities that Contractor and County shall perform.

Development and Test Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop and submit design for Development and Test Services.	X	
2. Review and approve design for Development and Test Services.		X
3. Develop and submit procedures for managing Development and Test environment to closely align with production.	X	
4. Review and approve procedures for managing Development and Test environment.		X

Development and Test Services Roles and Responsibilities		
5. Develop and submit management plan for capacity and moving workloads on and off.	X	
6. Review and approve management plan.		X
7. Develop and submit plans and design for hybrid cloud integration for Development and Test Services.	X	
8. Review and approve plans and design for hybrid cloud integration for Development and Test Services.		X
9. Design and submit a Development and Test Environment that is all virtual.	X	
10. Review and approve all virtual design.		X
Build Roles and Responsibilities	**Contractor**	**County**
11. Implement design for Development and Test Services.	X	
12. Implement procedures for managing Development and Test environment to closely align with production.	X	
13. Implement management plan for capacity and moving workloads on and off.	X	
14. Implement automated provisioning tools.	X	
15. Implement security architecture, as closely as possible, in the Development and Test environment.	X	
16. Implement full Identity Management Access for Development and Test Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
17. Manage all break-fix and Incidents in the Development and Test environment.	X	
18. Manage all workloads in the Development and Test environment for only work in progress is hosted	X	
19. Manage cold storage of virtual images not currently in use.	X	
20. Manage and support process to copy current production environment applications into the Development and Test Environment.	X	
21. Manage and provide all updates to Runbooks and other documentation for Portfolio Applications.	X	

Development and Test Services Roles and Responsibilities		
22. Manage all licenses needs to fully operate the Development and Test Environment.	X	
23. Manage the Development and Test Environment to ensure all work can be accomplished on schedule.	X	
24. Develop, manage and post the schedule for all work to be performed in the Development and Test Environment.	X	
25. Produce monthly reports on usage in the Development and Test Environment.	X	
26. Produce monthly reports on images and applications active and in cold storage in the Development and Test Environment.	X	

6.10. E-Mail Services

6.10.1. Overview

This section pertains to the Electronic Mail (E-Mail) Services Framework Component within the Data Center Framework. E-Mail is a critical service used by all County End-Users as a daily business, must-have productivity tool. E-Mail Services must ensure the safe and reliable uninterrupted delivery of E-Mail to County End-Users and external entities.

The E-Mail Services Framework Component applies to all Hardware, Software, services and policies needed to maintain and support E-Mail Services.

6.10.2. High Level Requirements

6.10.2.1. Contractor shall develop, for County approval, plans to migrate and upgrade E-Mail Services during Transition.

6.10.2.2. Contractor shall design, and deliver, for County approval, and implement a highly reliable, high redundant E-Mail Services platform that ensures zero data loss.

6.10.2.3. Contractor shall provide perimeter services that protect against SPAM and E-Mail Worms or malicious software of any sort.

6.10.2.4. Contractor shall design, deliver (for County approval) and implement secure E-Mail remote access (e.g. Outlook Web Access).

6.10.2.5. Contractor shall implement Microsoft Exchange for E-Mail Services.

6.10.2.6. Contractor shall maintain and upgrade Microsoft Exchange software versions within 12 months of major releases and within 3 months for minor releases.

6.10.2.7. Contractor shall establish and maintain global directory and synchronize E-Mail directories with all County Departments (e.g. Sheriff, District Attorney, SDCERA) or as specified by the County.

6.10.2.8. Contractor shall recommend a plan for County approval, and execute the approved plan for e-discovery services authorized by a Service Request.

6.10.2.9. Contractor shall integrate fax capabilities into E-Mail Services for End-Users.

6.10.2.10. Contractor shall recommend a plan for County approval, and execute the approved plan for DLP protection per County policies for E-Mail Services.

6.10.2.11. Contractor shall ensure and continuously update for each mailbox protection against any anti-malware and anti-spam or any other malicious product or vulnerability.

6.10.2.12. Contractor shall ensure that secure mobile access to E-Mail Services is provided to County-furnished or approved BYOD mobile devices.

6.10.2.13. Contractor shall apply County retention policy across all mailboxes without exception.

6.10.2.14. Contractor shall apply and provide unlimited mailbox storage for each mailbox.

6.10.2.15. Contractor shall recommend a plan for County approval, and execute the approved plan for in-place archiving on all mailboxes as an alternate storage location for historical messaging data (eliminate PST).

6.10.2.16. Contractor shall provide in-place hold to selected mailboxes, via Service Request, to preserve all mailbox items immutably for a specified period of time.

6.10.2.17. Contractor shall recommend a plan for County approval, and execute the approved plan for integrated digital signing to all mailboxes leveraging County PKI platform.

6.10.2.18. Contractor shall recommend a plan for County approval, and execute the approved plan for integrated encryption services on all mailboxes based on leveraging the County PKI platform.

6.10.2.19. Contractor shall ensure through continuous review and report that all End-User mailboxes comply with the County's E-Mail retention policy.

6.10.2.20. Contractor shall recommend a plan for County approval, and execute the approved plan for a more secure OWA solution that protects County Data and maintains simplified End-User interaction and authentication.

6.10.2.21. Contractor shall recommend a plan for County approval, and execute the approved plan to send encrypted E-Mails to E-Mail addresses outside of the County network.

6.10.2.22. Contractor shall recommend a plan for County approval, and execute the approved plan for the ability of external recipients of encrypted E-Mails with access to encrypted content via an authentication.

6.10.2.23. Contractor shall enable End-Users an expiration date for sent encrypted E-Mail messages.

6.10.2.24. Contractor shall provide self-help password administration for recipients of encrypted E-Mails that permit passwords to be established and reset.

6.10.2.25. Contractor shall ensure high delivery of cloud based E-Mail Services and complete End-User integration.

6.10.2.26. Contractor shall provide centralized support and tools for E-Mail Services hosted within the data center or hosted outside the data center.

6.10.2.27. Contractor shall maintain a timeline/roadmap of all E-Mail Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

6.10.2.28. Contractor shall maintain and be responsible for all components needed to provide E-Mail Services (e.g. load balancers, firewalls, IPS).

6.10.2.29. Contractor shall maintain E-Mail Services so there is not a single point failure thereby assuring County daily use continues to operate during any unplanned event or outage.

6.10.2.30. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to E-Mail Services.

6.10.2.31. Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security.

6.10.2.32. Contractor shall provide a Virtual Fax solution, which offers inbound fax capabilities to a group O365 mailbox, together with outbound fax capabilities from a group O365 mailbox.

6.10.2.33. Contractor shall also provide set up and porting services, when porting the analog number is possible, together with maintenance and break/fix.

6.10.3. Environment

6.10.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support E-Mail Services

6.10.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with E-Mail Services.

E-Mail Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit E-Mail Services operational and computing procedures.	X	
2. Review and approve E-Mail Services operational and computing procedures.		X
3. Produce and submit E-Mail Services architecture.	X	
4. Review and approve E-Mail Services architecture.		X
5. Produce and submit recommendations for E-Mail application standards on a yearly basis.	X	
6. Review and approve E-Mail application standards.		X
7. Produce and submit backup/recovery policies and procedures.	X	
8. Review and approve backup/recovery policies and procedures.		X
9. Produce and submit defining policies and procedures for functions including E-Mail, calendaring and mail messaging delivery components.	X	

E-Mail Services Roles and Responsibilities		
10. Review and approve policies and procedures for functions including E-Mail, calendaring and mail messaging delivery components.		X
11. Produce and submit plans to update and patch E-Mail Services to maintain reliability and security.	X	
12. Review and approve plans to update and patch E-Mail Services to maintain reliability and security.		X
13. Produce and submit procedures for directory synchronization with County departments.	X	
14. Review and approve procedures for directory synchronization with County departments.		X
15. Produce and submit plans and procedures to protect County End-Users from SPAM, E-Mail Worms or malicious software.	X	
16. Review and approve plans and procedures to protect County End-Users from SPAM, E-Mail Worms or malicious software.		X
17. Produce and submit End-User tip sheets on use of E-Mail Services.	X	
18. Develop procedures for E-Mail.	X	
19. Review and approve plans and procedures to allow County End-Users to encrypt E-Mails to external addresses.		X
20. Produce and submit End-User tip sheets on use of E-Mail Services including encryption.	X	
21. Review and approve for distribution End-User tip sheets on use of E-Mail Services.		X
22. Produce and submit plans for E-Mail integrated Fax solution.	X	
23. Review and approve E-Mail integrated Fax solution.		X
Build Roles and Responsibilities	**Contractor**	**County**
24. Design and implement E-Mail Services operational and computing procedures.	X	
25. Design, test and implement approved changes to the E-Mail application.	X	
26. Design, test and deploy E-Mail server refresh according to the approved plan.	X	

E-Mail Services Roles and Responsibilities		
27. Design and implement policies and procedures for functions including E-Mail, calendaring and mail messaging delivery components.	X	
28. Design, test and implement approved updates and patches to E-Mail Services.	X	
29. Design, test and implement directory synchronization with out-of-scope County departments.	X	
30. Design, test and implement approved plans and procedures to protect County End-Users from SPAM, E-Mail Worms or malicious software.	X	
31. Design, test and implement approved plans and procedures used by Data Center in order to allow County End-Users to encrypt E-Mail being sent to external addresses.	X	
32. Provide encryption plug-ins for Outlook clients.	X	
33. Deploy and install encryption profiles to E-Mail encryption End-Users.	X	
34. Implement approved backup/recovery policies and procedures.	X	
35. Distribute End-User approved tip sheets.	X	
36. Implement E-Mail retention policies.	X	
37. Design and implement E-Mail integrated Fax solution.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
38. Provide support, including break-fix, for all E-Mail Services Assets.	X	
39. Manage and support E-Mail Services to meet operational and computing procedures.	X	
40. Manage and support the E-Mail application.	X	
41. Support and provide E-Mail accounts to End-Users.	X	
42. Provide and support migration of End-User mailboxes in support of E-Mail server refresh or break-fix activity.	X	
43. Manage and support directory synchronization operations.	X	
44. Manage and support SPAM Services and other specific Services needed to protect End-Users.	X	

E-Mail Services Roles and Responsibilities		
45. Manage and maintain E-Mail accounts and E-Mail SMTP addresses.	X	
46. Manage and maintain E-Mail URL filtering Services to protect End-Users.	X	
47. Manage and support E-Mail encryption Services.	X	
48. Manage and maintain E-Mail Services to Service Levels.	X	
49. Perform backups on E-Mail Services Servers Assets as defined.	X	
50. Support E-Mail retention policies per County policy.	X	
51. Manage and support integrated Fax Services.	X	
52. Produce encryption resource unit reports monthly.	X	
53. Manage and Maintain E-Mail encryption accounts for End-Users.	X	

6.11. Unified Communications Infrastructure Services

6.11.1. Overview

This section pertains to the Unified Communications Infrastructure Services Framework Component within the Data Center Services Framework. The Unified Communications Infrastructure Services offering includes all the Framework Components needed to ensure enhanced, mobile, flexible, and more collaborative working environment through a single unified experience for County End-Users.

These Services include:

- Software deployment/management Services
- Management of distribution lists (DLs) and Unified Communication Integration Services (for example, presence management for User availability, voice/IM communications across multiple End-User devices, etc.)
- Acquisition, installation, upgrades, maintenance, support and tuning of collaborative computing Services (e.g., MS Exchange, Audio/Video and Web Conferencing etc.)
- Dedicated Real-Time Collaboration Services
- Synchronous Text Exchange
- Presence Awareness

- Peer-to-Peer Collaboration
- Audio/Video
- MS Lync
- Web Conferencing (Live Meeting)
- Mobile Support
- Utilization Reporting
- Federated Services shall be provided to external agencies approved by the County

The County currently uses Microsoft Office 365 Skype for Busines to provide Unified Communications Infrastructure Services

6.11.2. High Level Requirements

6.11.2.1. Contractor shall provide End-Users the ability to exchange text messages in real time (chat).

6.11.2.2. Contractor shall ensure the logging of any activity in Unified Communications Infrastructure Services shall be administratively disabled.

6.11.2.3. Contractor shall provide End-Users with presence capability.

6.11.2.4. Contractor shall provide End-User with the ability to share text, files, whiteboards and presentations.

6.11.2.5. Contractor shall provide all Unified Communications Infrastructure Services to County mobile devices.

6.11.2.6. Contractor shall provide scheduling of live meetings, web conferences, presentations for internal End-Users and external entities.

6.11.2.7. Contractor shall provide monthly utilization reports of all activity posted on the Service Portal.

6.11.2.8. Contractor shall integrate Unified Communication Infrastructure Services with Identity Access Management Services for all End-User authentication.

6.11.2.9. Contractor shall federate, per Service Request, any external entity into Unified Communication Infrastructure Services.

6.11.2.10. Contractor shall maintain and upgrade Unified Communication Infrastructure Services software versions within 12 months of major releases and within 3 months for minor releases.

6.11.2.11. Contractor shall provide integration for all Unified Communication Infrastructure Services with the E-Mail Services distribution lists.

6.11.2.12. Contractor shall maintain a timeline/roadmap of all Unified Communication Infrastructure Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.

6.11.2.13. Contractor shall maintain and be responsible for all components needed to provide Unified Communication Infrastructure Services (e.g. load balancers, firewalls, IPS).

6.11.2.14. Contractor shall maintain Unified Communication Infrastructure Services so there is not a single point failure thereby assuring County daily use continues to operate during any unplanned event or outage.

6.11.2.15. Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to Unified Communication Infrastructure Services.

6.11.2.16. Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security.

6.11.3. Environment

6.11.3.1. Hardware and Software

Contractor shall provide all Hardware and Software to support Infrastructure Services

6.11.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Unified Communication Infrastructure Services.

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop Unified Communications Infrastructure Services administration policies (including standards and procedures (new and/or updates) and review with the County.	X	
2. Produce and submit Unified Communications Infrastructure Services architecture.	X	
3. Review and approve Unified Communications Infrastructure Services architecture.		X
4. Review and approve/modify recommended/updated policies, standards and procedures.		X
5. Develop and document final operating procedures for all Unified Communications Infrastructure Services that meet the County requirements and adhere to defined policies and standards.	X	
6. Review and approve/modify final operating procedures documentation.		X
7. Define and submit collaborative computing services procedures.	X	
8. Review and approve collaborative computing services procedures.		X

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
9. Provide the County a briefing on upcoming trends in Unified Communications solutions on a regular basis.	X	
10. Identify process improvements to the Unified Communications service management function.	X	
11. Develop a failover plan for Unified Communications Infrastructure Services.	X	
12. Review and approve/authorize improvement recommendations		X
Build Roles and Responsibilities	**Contractor**	**County**
13. Procure and provision Unified Communications Infrastructure Services.	X	
14. Work with appropriate service delivery personnel to perform the installation, testing, and tuning of all technical environment hardware, software, peripherals and interfaces related to supporting Unified Communications Infrastructure Services platform.	X	
15. Deploy and manage Unified Communications Infrastructure Services, including post-deployment support and warranties.	X	
16. Perform end-to-end Incident determination and resolution for all Unified Communications Infrastructure Services related Incidents.	X	
17. Provide and support Remote Access Services for Unified Communications Infrastructure Services.	X	
18. Ensure that all activities affecting the Unified Communications Infrastructure Services environment(s) are coordinated and communicated through defined change management/change control processes and procedures.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
19. Support and participate in any upgrades or migrations and provide applicable services to upgrade infrastructure relating to Unified Communications Infrastructure Services platform.	X	
20. Manage, implement and coordinate all changes to the Unified Communications Infrastructure Services infrastructure.	X	

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
21. Create, maintain and provide all appropriate project plans, project time, technical specifications, management documentation and management reporting in a format that is acceptable to the County.	X	
22. Define monitoring requirements for Unified Communications Infrastructure Services.	X	
23. Develop and document monitoring procedures that meet requirements.	X	
24. Review and approve monitoring procedures.		X
25. Provide proactive and scheduled console monitoring of Unified Communications Infrastructure Services infrastructure and systems (e.g., Servers, Network and backups), respond to messages and take corrective action as required.	X	
26. Coordinate with technical support, Incident & Problem Management and Third-Parties in Incident & Problem resolution.	X	
27. Prepare reports on Unified Communications Infrastructure Services performance and review with the County.	X	
28. Administer the day-to-day interfacing with Third-Parties authorized by the County.	X	
29. Provide troubleshooting, repair and escalation of Incidents in the Unified Communications Infrastructure Services platform environment.	X	
30. Verify the integrity of all messaging backups/monthly restore tests.	X	
31. Ensure stability of the current environment is maintained during deployment of minor upgrades and software release maintenance, emergency software and/or hardware fixes/patches.	X	
32. Provide and utilize scheduling tools and processes for managing mailbox moves, archiving, and Unified Communications Infrastructure Services administration.	X	
33. Review and approve retention/backup/recovery requirements.		X

Unified Communication Infrastructure Services: Plan, Build and Operate Roles and Responsibilities		
34. Evaluate, coordinate and install patches as required to all Unified Communications Infrastructure Services (e.g., Hotfixes).	X	
35. Install service pack releases, as applicable.	X	
36. Check messaging logs, server logs and event monitoring.	X	
37. Provide and support Instant Messaging (IM) that utilize the Messaging system infrastructure and include a "Presence" status, application sharing, desktop sharing, and remote access functionalities.	x	
38. Provide technical assistance and subject matter expertise support as required by the County staff and Third-Party solution suppliers.	X	
39. Deploy software and systems that provide Unified Communications Infrastructure Services Services.	X	
40. Maintain (e.g., update to new releases, apply patches and fixes, etc.) Unified Communications Infrastructure Services software and systems. Perform activities or coordinate with appropriate parties.	X	
41. Perform break-fix support activities as required, remotely or on-site as needed.	X	

6.12. Storage Services

6.12.1. Overview

This section pertains to the Storage Services Framework Component within the Data Center Services Framework.

Storage Services is a Third-Party agnostic set of storage infrastructure based on the following three primary categories:

- Attached Storage – applies to direct attached storage, considered non-standard, used to meet Service Levels or to meet performance expectations
- SAN Storage - applies to a standard, centralized and consolidated storage environment

- Immutable Storage - applies to dedicated storage environment for maintaining a legal copy of records that are not modifiable or changeable

Storage Services includes, but are not limited to, End-User access, recovery (via backup and replication) of all Storage Services, data protection, storage availability, storage performance, storage reporting to the Business Group, low org or End-User, storage capacity analysis, and storage management. In addition, Storage Services includes, but are not limited to, storage consolidation, tiered storage, performance monitoring, archiving and replication.

Listed below are the specific tiers of storage definitions:

- Primary Tier –High Performance SAN used for Application Infrastructure Services
- Secondary Tier – Lower performing tier used for End-User data, replicated data (applications) and Infrastructure Services
- Archive Tier – archive storage based on age and inactivity Shared Storage Environment using low cost network storage devices .as approved by the County
- Immutable Tier –Immutable Storage using the replicated immutable storage devices as approved by the County
- Attached – direct connect storage
- Document Processing Center 1 – consists of two dedicated storage systems with 17TB Tier 1 Storage and 23 Tier 2 Storage, to support high throughput, imaging applications and will be located at a County Site
- Document Processing Center 2 – consist of two dedicated storage systems with 8TB Tier 1 Storage and 11 Tier 2 Storage, to support high throughput, imaging applications and will be located at a County Site

6.12.2. High Level Requirements

6.12.2.1. Contractor shall deliver dedicate Immutable Tier to the County.

6.12.2.2. Contractor shall develop plans, for County approval, and implement migration any attached storage used in the Application Infrastructure Services to SAN Storage.

6.12.2.3. Contractor shall support, manage and refresh DPC storage located at specific County Sites.

6.12.2.4. Contractor shall ensure all Application Infrastructure Services are integrated into SAN Storage.

6.12.2.5. Contractor shall develop and maintain a centralized, integrated, Storage Service solution for all County Data.

6.12.2.6. Contractor shall eliminate storage underutilization and avoid "islands of storage".

6.12.2.7. Contractor shall continuously decrease overall recovery times in Storage Services.

6.12.2.8. Contractor shall perform centralized management for Storage Services and in storage administration.

6.12.2.9. Contractor shall design, deliver, for County approval and implement separate storage environments for County Data and backup, replicated or mirrored data.

6.12.2.10. Contractor shall deliver dedicated, for County use only, Immutable Storage as part of the Storage Services.

6.12.2.11. Contractor shall measure and report Storage Services by installed, usable capacity.

6.12.2.12. Contractor shall not include any replicated, backup or DR data in the measurement of installed and usable capacity.

6.12.2.13. Contractor shall retain responsibility for storage related to backup and recovery.

6.12.2.14. Contractor shall maintain replication of Immutable Storage.

6.12.2.15. Contractor shall develop, deliver, for County approval, and implement processes to manage and control data growth across Storage Services.

6.12.2.16. Contractor shall develop, deliver, for County approval, and implement processes and controls for the elimination of unmanaged data growth.

6.12.2.17. Contractor shall increase storage, with County approval, in order to meet County business needs.

6.12.2.18. Contractor shall produce monthly Storage Services reports by storage tier down to the Business Group, department and End-User.

6.12.2.19. Contractor shall provide End-User self-service reporting and self-service management for Storage Services.

6.12.2.20. Contractor shall design, deliver, for County approval, and implement centralized control and management for Storage Services.

6.12.2.21. Contractor shall continuously implement plans, approved by the County, to lower storage costs to the County for Storage Services.

6.12.2.22. Contractor shall develop, deliver, for County approval, and implement plans to reduce down time due to data loss for Storage Services.

6.12.2.23. Contractor shall provide secure and bonded transportation and offsite storage of backups.

6.12.2.24. Contractor shall refresh Attached storage on the same cycle as the associated physical server.

6.12.2.25. Contractor shall refresh the Primary, Secondary and Archive tiers of storage on a five (5) year.

6.12.2.26. Contractor shall maximize the efficient use of storage throughout the Data Center Services to minimize and eliminate underutilization.

6.12.3. Environment

County Data included in the Storage Services environment shall be the following:

- County Portfolio Application
- End-User data

6.12.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Storage Services.

Storage Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommendations on Storage Services architecture.	X	
2. Review and approve recommendations on Storage Services architecture.		X
3. Produce and submit plans on Shared Storage Services consolidation and Application Server migration to Shared Storage Service environment on a yearly basis.	X	
4. Review and approve plans on Shared Storage and Data Management Services consolidation and Application Server migration to Shared Storage Service environment on a yearly basis.		X
5. Produce and submit Storage Services policies/procedures.	X	
6. Review and approve Storage Services policies/procedures.		X
7. Produce and submit Storage Services reporting policies/procedures.	X	
8. Review and approve Storage Services reporting policies/procedures.		X
9. Produce and submit Storage Services policies and procedures.	X	
10. Review and approve Storage Services policies and procedures.		X

Storage Services Roles and Responsibilities		
11. Produce and submit Storage Services refresh plan on a yearly basis.	X	
12. Review and approve Storage Services refresh plan on a yearly basis.		X
13. Produce and submit plans for meeting storage demands.	X	
14. Review and approve plans for meeting storage demands.		X
15. Produce recommendations for process improvement in backup and recovery for Storage Services Assets.	X	
16. Recommend and submit recovery policies/procedures for Storage Services Assets.	X	
17. Review and approve recovery policies/procedures for Storage Services Assets.		X
18. Produce and submit recommendation on capacity management.	X	
19. Review and approve recommendations on capacity management.		X
20. Produce and submit plans to add additional Storage.	X	
21. Review and approve plans to add additional Storage.		X
22. Produce and submit a data management strategy that make certain that commonly used data has a defined minimum set of characteristics that include the following: • Definition of the data object (what is it?) • Reference (where and how is the data object used?) • Metadata (data object attributes, such as type, size, and range of values) • Ownership and governance (who owns data, definitions, content, and so on?)	X	
23. Review and approve data management strategy.		X
24. Implement that strategy using an Information Lifecycle Management (ILM) approach for storing County Data.	X	

Storage Services Roles and Responsibilities		
25. On an initial and ongoing basis, evaluate the County's data to identify redundancies, excess capacity, and opportunities for data consolidation using strategies such as data warehousing and data archiving and reduce data storage costs through the following: • Leveraging centralized hardware • Reducing administrative costs by reducing the number of databases • Providing centralized data repository • Reducing costs by reducing under-utilized storage • Reducing and eliminating autonomous backup and recovery solutions for centrally administered and managed backup and recovery	X	
26. Plan and schedule all storage-related software/driver/microcode/etc. patching and upgrades.	X	
Build Requirements, Roles and Responsibilities	**Contractor**	**County**
27. Design and Implement recovery processes based on approved policies/procedures.	X	
28. Design and Implement Storage Services management processes based on approved policies/procedures.	X	
29. Implement Storage Services Reporting.	X	
30. Design and Implement storage consolidation based on approved recommendations.	X	
31. Deploy, manage, communicate and report on activities related to Storage Services refresh.	X	
32. Review and approve Storage Services refresh report.		X
33. Design and Implement Storage Services provisioning and allocation processes based on approved policies.	X	
34. Design and implement capacity management.	X	
35. Implement approved Storage Services policies and procedures.	X	
36. Implement necessary physical and logical security to protect the County's data (e.g. through access controls, storage network, and host-based allocation controls, SAN zoning and host/array-level logical unit (LUN) masking).	X	
Operate Requirements, Roles and Responsibilities	**Contractor**	**County**

Storage Services Roles and Responsibilities		
37. Provide support, including break-fix, for all Storage Services Assets.	X	
38. Manage and affect the appropriate resolution of Incident events until the operation of the storage is returned to normal by following customized procedures as well as resolving Incidents upon an automated or manual detection of an event related to storage components.	X	
39. Manage and support the Storage Services.	X	
40. Produce and submit monthly Storage Services reports.	X	
41. Review and approve monthly Storage Services reports.		X
42. Support Storage Services refresh.	X	
43. Perform and support media management activities for Storage Services.	X	
44. Manage and support the media requests.	X	
45. Provide data storage Services (e.g., RAID groups, storage pools, LUNs; presenting — masking and zoning; reclamation; optimization — tiers, deduplication, thin provisioning, etc.).	X	
46. Perform tapes mounts as required.	X	
47. Perform special tape shipments as requested.	X	
48. Provide options for on-premises and offsite data backup storage.	X	
49. Provide backup and restore options such as the possibility to self-restore.	X	
50. Load and manage Third-Party media as required.	X	
51. Prepare and manage media for use by microfiche service.	X	
52. Manage and perform file transfers and other data movement activities related to break-fix or consolidation of Storage Services Assets.	X	
53. Perform data backups of Storage Services per approved policies and procedures.	X	
54. Perform recovery processes on Storage Services Assets.	X	
55. Perform storage utilization management.	X	
56. Manage and maintain all Storage Services Assets and Services.	X	

Storage Services Roles and Responsibilities		
57. Manage and maintain backup media library.	X	
58. Manage and maintain the Storage Services Assets.	X	
59. Produce and submit Storage Services Management Reports.	X	
60. Review and accept Storage Services Management Reports.		X

6.13. Backup and Recovery Services

6.13.1. Overview

Backup and Recovery Services are the activities associated with providing ongoing Backup and Recovery according to County schedules and requirements. Contractor must demonstrate that it consistently meets or exceeds County's ongoing Backup and Recovery requirements. All Hardware, all Software and all storage (online, near online, and offline) used for any backup and recovery Services are Contractor-provided.

6.13.2. High Level Requirements

6.13.2.1. Contractor shall perform backups on all County Data.

6.13.2.2. Contractor shall develop management plan that contains procedures for monitoring backup infrastructure, for ensuring successful backup and recovery job completion, for complying with change management process and for testing restore process.

6.13.2.3. Contractor shall maintain a complete inventory of all existing backup equipment including, backup servers and clients, automated libraries, backup media and storage networking components.

6.13.2.4. Contractor shall provide centralized backup and recovery policy management.

6.13.2.5. Contactor shall support disk-based backup target.

6.13.2.6. Contractor shall provide provision for auto discovery of virtual servers.

6.13.2.7. Contractor shall provide single-pass image backup of virtual servers.

6.13.2.8. Contractor shall provide integrated authentication and LDAP services.

6.13.2.9. Contractor shall support Oracle RMAN integration.

6.13.2.10. Contractor shall provide volume shadow copy service (VSS).

6.13.2.11. Contractor shall support full and incremental backups.

6.13.2.12. Contractor shall provide file and virtual server image restore capability.

6.13.2.13. Contractor shall provide ability to customize retention period by policy

6.13.2.14. Contractor shall support application quiesce.

6.13.2.15. Contractor shall support file include/exclude functionality.

6.13.2.16. Contractor shall support data that resides in cloud infrastructure Contractor shall provide point-in-time file and object recovery.

6.13.2.17. Contractor shall perform continuous capacity planning in the Backup and Recovery Services environment to address data growth.

6.13.2.18. Contractor shall implement a NetBackup solution for Tulsa and San Diego sites with replication of immutable copies in Colorado Springs for Disaster Recovery. The Netbackup solution shall also provide daily backup of the AWS West Commercial tennant, with daily replication to the AWS East Commercial immutable tenant for disaster recovery.

6.13.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Backup and Recovery Services.

Backup and Recovery Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Backup and Recovery schedules, requirements and policies.		X
2. Recommend standard practices for Backup and Recovery Services strategies, policies, and process and procedures.	X	
3. Develop, document and maintain in the Standards and Procedures Manual the Backup and Recovery schedules and procedures that adhere to County requirements and policies.	X	
4. Coordinate the Backup and Recovery Standards and Process and Procedure Manual with County Security and Legal teams.	X	
5. Review and approve Backup and Recovery schedules and process and procedures.		X
Build Roles and Responsibilities	**Contractor**	**County**
6. Define Backup and Recovery Monitoring and Reporting requirements and policies.	X	
7. Review and approve Backup and Recovery Monitoring and Reporting procedures.		X
Operate Roles and Responsibilities	**Contractor**	**County**
8. Provide and Manage backup media inventory (tape, disk, optical and other media type) including the ordering and distribution of media.	X	
9. Perform Framework Component backups and associated rotation of media as required.	X	
10. Identify and establish a secure off-site location for data media.	X	
11. Approve secure off-site location for data media.		X
12. Archive data media at a secure off-site location.	X	
13. Ensure ongoing ability to recover archived data from media as specified (backward compatibility of newer backup equipment).	X	

Backup and Recovery Services Roles and Responsibilities		
14. Test backup media to ensure incremental and full recovery of data is possible and ensure integrity, as required or requested by County.	X	
15. Recover files, file system or other data required from backup media, as required or requested by County.	X	
16. Provide recovery and backup requirements and updates as they change.		X
17. Provide County access to backup and recovery reporting and monitoring systems and data.	X	

6.14. Managed Print Services

6.14.1. Overview

This is the section pertains to the Managed Print Services Framework Component within the Data Center Framework. The Managed Print Services Framework Component applies to all the Hardware, Software and services needed to maintain and support managed print. Services provided by the Contractor are print and output facilities, print output operations, operating printer devices, distributing printed output, replenishing consumable materials, preparing and managing media for use by microfiche service and repairing printer devices

6.14.2. High Level Requirements

6.14.2.1. Maintain reliable Managed Print Operations that allows County business to continue uninterrupted.

6.14.2.2. Lower overall Managed Print cost by increasing overall efficiencies.

6.14.3. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Managed Print Services.

Managed Print Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Managed Print Services Roles and Responsibilities		
1. Produce and submit output management requirements, policies, and procedures including transport, delivery locations and schedule requirements.	X	
2. Review and approve output management requirements, policies, and procedures.		X
3. Produce and submit automated output distribution requirements.	X	
4. Review and approve automated output distribution requirements.		X
5. Produce and submit recommendations for using distributed printing methodologies and technologies to update and modernize Managed Print Services.	X	
6. Review and approve recommendations for using distributed printing methodologies and technologies to update and modernize Managed Print Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
7. Design and implement output management requirements, policies, and procedures including transport, delivery locations and schedule requirements.	X	
8. Design, test and implement approved automated output distribution requirements.	X	
9. Design, test and implement approved recommendations for modernizing the Managed Print Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
10. Provide support, including break-fix, for all Managed Print Assets.	X	
11. Provide print output (including both paper and microfiche) facilities for the County.	X	
12. Perform and manage print output (including both paper and microfiche) distribution and delivery to specified County locations.	X	
13. Separate and organize printed output materials (including both paper and microfiche) and place into designated bins at the designated delivery points.	X	
14. Store preprinted check stock in a secure document vault in Contractor secured print facility.	X	

Managed Print Services Roles and Responsibilities		
15. Ensure that output devices are functioning, including performing or coordinating maintenance and meet or exceed Service Levels.	X	
16. Store and manage consumables, such as paper, special forms, check stock, print ribbons, ink, tapes, etc. Ensure that special forms and check stock are current and adequately stocked every Month. Coordinate acquisition of additional materials as needed.	X	
17. Provide microfiche Services.	X	

6.15. Public Key Infrastructure (PKI) Services

6.15.1. Overview

This section pertains to the Public Key Infrastructure (PKI) Services Framework Component of the Data Center Services Framework. PKI Services infrastructure supports and manages all the keys and certificates, the distribution and identification of public encryption keys, enabling End-Users and devices to both securely exchange data, securely connect to the County internal network, digital signatures and verify identity. The PKI Service consists of Hardware, Software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates.

County currently uses Symantec Managed PKI Service to deliver the PKI Service.

6.15.2. High Level Requirements

6.15.2.1. Contractor shall develop additional use cases for the expansion of PKI Services.

6.15.2.2. Contractor shall develop and implement device authentication strategies based on PKI Services.

6.15.2.3. Contractor shall develop and implement End-User authentication methodologies based on PKI Services.

6.15.2.4. Contractor shall use PKI Services for all applications of digital signature.

6.15.2.5. Contractor shall maintain currency on PKI Services.

6.15.2.6. Contractor shall deploy enterprise self-enrollment for PKI Services hosted on the Service Portal.

6.15.2.7. Contractor shall act as the Policy Authority for PKI Services.

6.15.2.8. Contractor shall be responsible for Certificate Practices Statements in the operation of PKI Services.

6.15.2.9. Contractor shall manage the root CA as a public PKI.

6.15.2.10. Contractor shall manage the entire lifecycle of all certificates used in the PKI Service.

6.15.2.11. Contractor shall establish monthly reporting methodology to track usage of certificates across the entire lifecycle.

6.15.2.12. Contractor shall maintain and establish integration with infrastructure supporting the Services (e.g. mobile device management, software distribution, authentication services).

6.15.2.13. Contractor shall maintain a browser agnostic solution for PKI Services.

6.15.2.14. Contractor shall ensure PKI Services is a valid and certified certificate authority externally.

6.15.2.15. Contractor shall maintain an accurate and up-to-date inventory of PKI Services.

6.15.2.16. Contractor shall design and standardize, with County approval, PKI Services.

6.15.2.17. Contractor shall maintain public key certificates for End-Users and devices.

6.15.2.18. Contractor shall maintain a certificate repository.

6.15.2.19. Contractor shall implement certificate revocation procedures and provide key backup and recovery.

6.15.2.20. Contractor shall maintain support for non-repudiation of digital signatures

6.15.2.21. Contractor shall maintain currency on PKI Services to the latest versions and releases.

6.15.2.22. Contractor shall implement automatic update of key pairs and certificates.

6.15.3. Environment

6.15.3.1. Support

The following is a list of items currently supported or future support by PKI Services:

6.15.3.1.1. Secure Remote Access – strong authentication for Remote Access

6.15.3.1.2. Secure network access - transparent authentication to Wi-Fi access points

6.15.3.1.3. Secure E-Mail – digitally signed, encrypted E-Mail Services

6.15.3.1.4. Strong web authentication – authentication services to web apps and pages via browser

6.15.3.1.5. Document signing – digitally signed Adobe PDF documents

6.15.4. Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with PKI Services.

PKI Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop and submit annually additional use cases for the expansion of PKI Services.	X	
2. Review the additional use cases.		X

PKI Services Roles and Responsibilities		
3. Develop and submit device and End-User authentication plans.	X	
4. Review and approve device and End-User authentication plans.		X
5. Develop, maintain and submit operational procedures and End-User instructions.	X	
6. Review and approve operational procedures and End-User instructions.		X
7. Develop and submit plans to integrate PKI Service into E-Mail Services.	X	
8. Review and approve plans to integrate PKI Service into E-Mail Services.		X
Build Roles and Responsibilities	**Contractor**	**County**
9. Implement designs and plans to PKI Services.	X	
10. Implement certificate lifecycle and self-service capabilities on the Service Portal.	X	
11. Implement integration of PKI Service into E-Mail Services.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
12. Develop and submit monthly reports on PKI Services.	X	
13. Manage CA Root.	X	
14. Support and maintain certificate lifecycle and self-service capabilities.	X	
15. Maintain CSP statements.	X	
16. Maintain currency of PKI Services.	X	
17. Support authentication of mobile devices.	X	
18. Support E-Mail Service use of PKI Services.	X	

7. APPLICATIONS SERVICES

7.1. Overview

Applications Services consists of three separate sets of requirements, roles and responsibilities:

- Applications Maintenance and Operations (M&O) Services – support for Applications in production
- Applications Development Services – development of new software
- Electronic Health Records (EHR) Program Management Services – support for existing EHR and implementation of additional EHR capabilities.

7.2. Application Maintenance and Operations Services

7.2.1. Overview

M&O Services consist of any one-time and ongoing maintenance, operations, support, planning, management, administrative support, oversight, tuning, planning, and any other Services that are either direct or incidental, ancillary, customary, or necessary to perform the activities described below. The Contractor is responsible to support and maintain all environments and systems required to support Portfolio Applications.

7.2.2. High Level Requirements

7.2.2.1. Contractor shall restore Services in accordance with Service Levels.

7.2.2.2. Contractor shall operationally maintain all Portfolio Applications in production with high availability and performance.

7.2.2.3. Contractor shall ensure all maintenance, development and integration activities are aligned with County architecture standards, guiding principles, architecture bricks and patterns.

7.2.2.4. Contractor shall be responsible for performing work on Incidents (e.g. development, test, training, etc.) and production environments, middleware or any needed components to provide M&O Services for Portfolio Applications.

7.2.2.5. Contractor shall maintain accurate and continuous prompt updates to asset and system documentation.

7.2.2.6. Contractor shall ensure cross Framework integration and communication is conducted for Application Incidents, outages, maintenance work, planning purposes and all changes.

7.2.2.7. Contractor shall provide Services in alignment with ITIL and CMMI standards to ensure predictable, repeatable and successful results.

7.2.2.8. Contractor shall implement new patches and versions (within the current release), prioritizing patches that address security vulnerabilities.

7.2.2.9. Reserved.

7.2.2.10. Contractor shall include all services (e.g., labor), software, hardware, and required system environments.

7.2.2.11. Applications M&O Services do not include programming any additional functionality beyond what is included in new patches and dot releases. Contractor shall perform maintenance Services that include Preventative, Adaptive and Perfective Maintenance as described below:

7.2.2.11.1. Preventive Maintenance

Contractor shall perform preventive maintenance Services to diagnose and correct latent defects and other known errors in the Applications. Contractor is required to provide preventive maintenance that covers events that, if not addressed proactively, may affect Applications in production.

7.2.2.11.2. Adaptive Maintenance

Contractor shall perform adaptive maintenance Services so that Application performance is not affected by changes to interfacing Applications or new Applications or packages and infrastructure

changes that, if not addressed proactively, have the potential to impact Applications in production.

7.2.2.11.3. Perfective Maintenance

Contractor shall perform perfective maintenance Services to optimize performance of the Applications, with particular focus on areas including: general performance tuning (e.g., to improve Application response time), database performance tuning (e.g., storage space, query refinement), etc. Tool and script development to make the Maintenance Services more productive or labor saving is also included in this category.

7.2.3. Roles and Responsibilities

Contractor shall perform the Applications M&O Services described in the overview, high level requirements, descriptions and tables in the sections below. The sections below describe in more detail the requirements, roles and responsibilities in the plan, build and operate format for each specific section.

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Application M&O Services requirements and policies.		X
2. Provide recommendations for archiving, performance tuning, patching, database administration, and Application onboarding/retirement.	X	
3. Provide recommendations for preventive, adaptive, and perfective maintenance.	X	
4. Provide recommendations on operational procedures.	X	
5. Review and approve Contractor recommendations on M&O processes, procedures, maintenance (preventive, adaptive, perfective), and Application onboarding/retirement.		X
6. Provide recommendations for upgrade, system changes, Applications architecture changes or anything else that can affect the operational integrity of the Applications.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
7. Provide annual portfolio analytics on production Applications, including technical obsolescence (at a component level, where applicable), defect rates, and costs by Application.	X	
8. Monitor technical trends through independent research; document and report on products and Services.	X	
9. Participate in annual technical and business planning sessions to establish standards, architecture and project initiatives.	X	
10. Define authorization requirements for End-Users, roles, schemas, etc. and approve change requests.	X	
11. Define job schedules for sequencing and run times.	X	
Build Roles and Responsibilities	**Contractor**	**County**
12. Perform pre-production execution simulation.	X	
13. Provide Services in alignment with ITIL, CMMI standards or other leading practices to result in predictable, repeatable, and successful results.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Update the Standards and Procedures Manual with County-approved procedures and standards.	X	
15. Conduct periodic reviews of configuration documentation for accuracy.	X	
16. Provide a documented list of items to be addressed for consideration as part of future upgrades.	X	
17. Validate and provide Application-related Service Desk scripts are updated and accurate.	X	
18. Approve Service Desk script updates.		X
19. Provide planning and schedules for new Applications supported by M&O Services for a system or change placed into production. M&O shall perform M&O Services after the system is placed into production unless otherwise directed by the County.	X	
20. Approve M&O Services to support a new system or change in production.		X
21. Develop and maintain Application version and release Roadmap for all software and tools for each Portfolio Application.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
22. Provide portfolio report for County review of past month Incidents that impacted Application operations.	X	
23. Provide cost and labor hour information at the PA-ID level to facilitate annual portfolio rationalization and support monthly cost allocation to departments.	X	
24. Perform business planning for capacity and performance.		X
25. Provide input into defining requirements for all Applications Development projects to be transitioned to Applications M&O.	X	
26. Recommend potential improvements to Application security architecture.	X	
27. Identify possible product and software tool enhancement opportunities for improved performance and potential cost savings.	X	
28. Recommend potential improvements to Application security.	X	
29. Review and approve improvements to Application security.		X
30. Perform preventive, adaptive and perfective maintenance based on County-approved procedures.	X	
31. Perform archiving, performance tuning, patching, database administration based on County-approved procedures.	X	
32. Perform system log storage and management.	X	
33. Perform root cause analysis resulting from an Incident.	X	
34. Identify and resolve locking conflicts, latch contention, rollback requirements, etc. for all database instances as it pertains to maintenance activities.	X	
35. Retire Applications (performing tasks based on retirement procedures in the Standards & Procedures Manual) as approved by the County.	X	
36. Perform necessary tasks to remedy risks and Incidents identified in the weekly Application and database performance and capacity reports.	X	
37. Create/refresh development/test databases from production data to support O&M activities according to a pre-scheduled cycle.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
38. Monitor and execute production jobs and perform associated interventions (e.g., restarting jobs, re-running jobs.)	X	
39. Review and approve changes that alter or impact the production system and Application.		X
40. Restore Applications following an outage or Incident.	X	
41. Perform triaging and investigation of Incidents regardless of whether these result in an enhancement in the future or impact other Service Frameworks.	X	
42. Perform code fixes to resolve Incidents that stop, slow or hold-up Application processes.	X	
43. Perform general Application administration.	X	
44. Perform routine system patching (e.g., monthly/quarterly/annual) to keep the system current.	X	
45. Perform prompt updates of system documentation.	X	
46. Perform prompt updates of current code in source code repository.	X	
47. Track trends on Incidents to identify systemic Problems to be reported to the County and corrected by the Contractor.	X	
48. Maintain current non-production environments and keep the system operational for M&O requirements.	X	
49. Provide unplanned maintenance including activities to restore service as initiated by Incident tickets that have been initiated by County Users, or Contractor or Third-Parties.	X	
50. Perform analysis, design, coding, testing, data conversion, documentation, End-User coordination and communication, and production turnover activities and the management of these activities for restoration of service.	X	
51. Perform triage support by determining if the Incident is an Application Incident vs. another Framework or a Third-Party Incident.	X	
52. Support Incident and Problem management including RCAs.	X	
53. Coordinate with Third-Parties for patch installation and support for restoration of service.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
54. Provide updates to existing documentation regarding steps necessary to restore service.	X	
55. Provision and de-provisioning all and any accounts that are authorized to be created, changed or modified for Portfolio Applications authentication and authorization.	X	
56. Includes Third-Party patch installation and support to restore service, including all patches that address fixes to known defects and associated security vulnerabilities. If a patch only includes new functionality, it shall be installed under Applications Development Services. If a patch includes both known defects/security vulnerabilities and new functionality, it shall be implemented under Applications Maintenance and Operations Services.	X	
57. Participate in change review control board activities.	X	
58. Proactively evaluate, identify and recommend configurations or Changes to configurations to enhance performance.	X	
59. Update and maintain information and data in the Unified Asset Management System.	X	
60. Establish and maintain configuration and system parameters in a consistent manner across like server environments.	X	
61. Execute processes for the proper maintenance and functioning of Interfaces (e.g., initialization parameter, load balancing, tuning, configuration management).	X	
62. Coordinate communications with Third-Parties and manage the information exchange with interfaces.	X	
63. Perform upgrades to Third-Party software or tools, including operating systems or database software.	X	
64. Perform changes to ensure non-production environments are using same versions, updated code and system features as production.	X	
65. Perform regression testing of Application when an enhancement (e.g., service pack release) or change in code is performed.	X	
66. Conduct Application testing in non-production environments.	X	
67. Perform triage to engage Third-Party, troubleshooting, Application of patches and/or other types of fixes.	X	

Maintenance and Operations Services: Plan, Build and Operate Roles and Responsibilities		
68. Maintain and execute a release management schedule.	X	
69. Perform special testing for events, e.g., public holidays, end of financial year, end of calendar year, daylight savings time.	X	
70. Provide, maintain and update the Portfolio Application Identification (PAID) report of active, inactive and inactive-retain Applications.	X	

7.2.4. Application Programming

Application programming Services are the activities associated with the programming, scripting, configuring or customizing of Application modules to support Maintenance and Operations of the production Application Portfolio.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Application Programming as part of Applications M&O Services.

Application Programming Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Review County's existing technical standards (e.g., naming, JCL, etc.).	X	
2. Recommend programming (coding), development, and technical documentation policies, procedures, and standards for inclusion in the Standards and Procedures Manual.	X	
3. Review and approve overall programming, development, and technical documentation in the Standards and Procedures Manual.		X
Build Roles and Responsibilities	**Contractor**	**County**
4. Create working directories to store source code in the enterprise code version manager or repository.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
5. Maintain all current versions of custom code in the approved code repository managed by the Contractor.	X	

Application Programming Services: Plan, Build and Operate Roles and Responsibilities		
6. Recommend modifications and performance-enhancement adjustments to system software and utilities based on County performance standards.	X	
7. Manage all programming and development efforts using industry-standard project management tools and methodologies.	X	
8. Perform all software engineering activities using industry best practices.	X	
9. Employ standard software engineering practices to promote consistency and maintainability.	X	
10. Conduct planned status reviews and provide written report on results to County.	X	

7.2.5. Application Integration and Testing

Application integration and testing are the Services associated with the confirmation that the individual Application Framework Components work together properly and, as a whole, perform their specified functions. This includes Interfaces to other Applications already in production at, or developed by, County or Third-Parties as stated in the applicable requirements documents.

The following table identifies the Application Integration and Testing Services that the Contractor shall perform.

Application Integration and Testing Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop, document and maintain in the Standards and Procedures Manual integration and testing procedures that meet County requirements and adhere to policies defined by County.	X	
2. Review and approve changes to the Standards and Procedures Manual for testing.		X
3. Develop an overall test plan that documents the test strategy, coverage, scenarios, test bed, test data, methods, schedule and responsibilities to accomplish integration and testing.	X	
4. Approve test plan.		X
Build Roles and Responsibilities	**Contractor**	**County**

Application Integration and Testing Services: Plan, Build and Operate Roles and Responsibilities		
5. Provide a test bed with real-time production data.	X	
6. Mask sensitive information in tests that use production data.	X	
7. Create test cases with appropriate use of County-provided data for generating test data to perform all appropriate testing, e.g., unit testing, end-to-end testing, stress testing, regression testing.	X	
8. Create test scenarios to test end-to-end business cases.	X	
9. Create test environment and data where required for support, enhancements or projects, including demonstration of requirements traceability to verify requirements have been satisfied.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
10. Conduct testing per test plan requirements.	X	
11. Facilitate and support User acceptance test as agreed-upon with the County, e.g., establish adequate test environment based on User acceptance criteria, prepare data to support test scenarios within modified system, manage the relationship with all interfaced systems necessary to conduct test, perform troubleshooting, simulate interfaces or working with integrated systems to conduct end-to-end testing, support batch processing, exercise functionality and report results.	X	
12. Conduct User acceptance test.		X
13. Manage the County functional, Integration test, and Regression Testing environments and associated test data, including creation and maintenance during the testing period.	X	
14. Provide shared access to the mutually agreed-upon defect tracking tool for the purpose of allowing County to initiate, track, and report County-identified defects (e.g., User acceptance testing).	X	
15. Correct defects found as a result of testing efforts.	X	
16. Stage systems before implementation into production.	X	
17. Support County for functional and non-functional testing of Applications to confirm systems are functioning as expected after infrastructure changes have been implemented.	X	
18. Maintain software release matrices across development, quality assurance and production environments and networks.	X	

Application Integration and Testing Services: Plan, Build and Operate Roles and Responsibilities		
19. Conduct Integration test and security testing for all new and upgraded Application software, including the associated equipment and networks to include Unit testing, system, Integration test and Regression testing based on requirements defined in requirements and design documents.	X	
20. Assess and communicate the overall impact and potential risk to components prior to implementing Changes.	X	
21. Stage new and upgraded software or services to seamlessly transition into existing environment based on requirements defined in requirements and design documents.	X	
22. Perform Configuration Management and Change Management activities related to integration and testing.	X	
23. Review and approve test results.		X
24. Manage and support software and test data in test environments.	X	
25. Ensure testing results are in compliance with policies, procedures, plans, and test criteria and metrics (e.g., defect rates, progress against schedule).	X	
26. Define test-to-production turnover requirements and instructions for each Project or release.	X	
27. Approve test-to-production turnover requirements and instructions.		X
28. Produce and submit reports on results from test-to-production activities if applicable.	X	
29. Review and approve reports on test-to-production results.		X
30. Perform software support to migrate code from test to production as approved by the County.	X	
31. Track migration status and notification.	X	

7.2.6. Application Implementation and Data Migration

Application implementation and data migration Services are the activities associated with the installation and migration of new or upgraded components to the production environment. In addition, these include Services to localize new or upgraded components so that they adhere to local business practices as well as legal, regulatory and statutory needs.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Applications that receive patches, version upgrades, or other changes.

Application Implementation and Data Migration Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Create an implementation plan outlining the scope, approach and execution planned for the deployment of new/enhanced Applications and/or the migration of Applications into M&O Services.	X	
Build Roles and Responsibilities	**Contractor**	**County**
2. Perform data migration from existing systems to new systems, by either electronic or manual methods.	X	
3. Produce and submit operations and administration procedures related to code migration (e.g. CRCB documents, code version check in, etc.).	X	
4. Review and approve operations and administration procedures related to code migration.		X
Operate Roles and Responsibilities	**Contractor**	**County**
5. Coordinate and assist with deployment and support activities with County and/or its designees as directed by County.	X	
6. Develop data migration plans and scripts for use or execution by County, whether from existing systems to new systems, by either electronic or manual methods as required.	X	
7. Execute data migration plan by moving data into the production environment.	X	
8. Develop, document and maintain in the Standards and Procedures Manual implementation and migration procedures that meet requirements and adhere to policies defined by County.	X	
9. Coordinate and review all implementation and migration plans, in accordance with Change Management policies.	X	
10. Upon County request and approval install new or enhanced components (e.g., software, middleware, utilities, configurations) within the development environment.	X	

Application Implementation and Data Migration Services: Plan, Build and Operate Roles and Responsibilities		
11. Upon County approval, within the development environment, perform Application Services Framework Component upgrades as a result of new and enhanced architectures and County upgrade plans and requirements (e.g., Hardware, Software, middleware, utilities, networks, peripherals, configurations).	X	
12. Coordinate implementation and migration support activities with County.	X	
13. Within the development environment, perform Application and/or data migration and conversion by electronic or manual methods (e.g., upgraded databases, address tables, management information bases).	X	
14. Attend and seek change control review board approval, or any other procedures required to obtain approval to implement a change into production environment.	X	
15. Create "go-live" checklist and conduct the "go/no-go" meetings	X	
16. Approve production implementation, go-live checklist and "go/no-go" decisions.		X
17. Deploy system.	X	

7.2.7. Application Documentation

Contractor shall develop and maintain documentation for all Applications, including:

- System specifications and documentation
- Solution design documentation
- System security plans
- End-User documentation
- Updates and release notes
- Run-book data and documentation

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Applications Documentation.

Application Documentation Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**

Application Documentation Services: Plan, Build and Operate Roles and Responsibilities		
1. Recommend specifications and documentation format and content per County requirements.	X	
2. Approve documentation format and content.		X
3. Provide system specifications and technical documentation.	X	
4. Provide operational processing flow.	X	
5. Provide system installation, support, configuration and tuning documentation.	X	
6. Provide Application hardware and system Software requirements documentation.	X	
7. Provide documentation for Applications on patches, updates and release notes.	X	
8. Provide solution design documentation.	X	
9. Review and approve all Applications documentation.		X
Build Roles and Responsibilities	**Contractor**	**County**
10. Maintain, and provide County access to, physical and logical on-line libraries of all deliverables and documentation produced in the course of performing Applications work (e.g., specifications, process flows, User manuals, operating manuals).	X	
11. Prompt update documentation to be current and accurate in all relevant system of records (e.g., AppsManager, Service Desk Scripts, Solution Design Documents).	X	
12. Prompt update of code version manager tool set with updated code that is created or changed. The code repository managed by the Contractor must be accurate and current.	X	
13. Validate documentation is promptly updated and coding standards are followed.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
14. Provide system and Application security procedures.	X	
15. Provide standard operating procedures in support of Application characteristics and features.	X	
16. Prepare updates and release notes.	X	
17. Document version control for all documentation.	X	

Application Documentation Services: Plan, Build and Operate Roles and Responsibilities		
18. Assist County in developing an Application Disaster Recovery process and the associated documentation.	X	
19. Approve documentation.		X

7.2.8. Application Training

Following Transition and after each implementation, Contractor shall conduct all the necessary training programs for Contractor Personnel to preserve and enhance the knowledge and understanding of the Applications. It is the Contractor's responsibility to maintain this proficiency for replacement Contractor Personnel at no additional cost to the County. Contractor shall provide base training to key County personnel when Contractor develops a new functionality.

Contractor shall share with County the experience that Contractor has gained from daily Incident handling via knowledge sharing sessions, best practices sessions, training programs, etc., to improve the overall knowledge base of the Applications. Contractor shall provide County with copies of all instructor manuals and other training materials created or used by Contractor Personnel in conducting such training.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Application Training.

Application Training Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop training plan.	X	
2. Approve training plan.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Update technical training materials.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide technical training assistance and knowledge transfer to existing County support personnel, during deployment as requested.	X	
5. Provide training materials related to the technical aspects of Applications to County as applicable.	X	

Application Training Services: Plan, Build and Operate Roles and Responsibilities		
6. Support County's training of its Service Desk agents, including supporting County's development of dialogue scripts.	X	
7. Develop, document and maintain in the Policies and Procedures Manual Training and knowledge transfer procedures that meet County's requirements and adhere to policies defined by County.	X	
8. Develop and deliver training program to instruct County personnel on the provisions included within the Services (e.g., "rules of engagement," how to request Services).	X	
9. Develop and implement knowledge transfer procedures so that key County staff understand key components of the Enhancements and/or Deliverables.	X	
10. Develop, document and deliver training requirements that support the ongoing provision of the Services, including refresher courses as needed and instruction on new functionality.	X	

7.2.9. Application Quality Assurance Services

Contractor shall provide the Quality Assurance (QA) Services with respect to all Applications created or enhanced as part of this Agreement. QA Services are a systematic, planned set of actions necessary to provide confidence that the Software update/development processes conform to established functional technical requirements as well as with the managerial requirements of keeping the schedule and resources within budgetary confines. Contractor shall provide County with appropriate visibility into the QA Services processes that Contractor uses and of the results as related to the Application being worked upon.

Contractor shall support and suggest improvements for all QA Services conducted and processes adopted by County.

Contractor shall perform the QA Services throughout the entire Software Development Life Cycle (SDLC). QA Services include the following:

- A quality management approach
- Effective software engineering technology (methods and tools)
- Formal technical reviews applied throughout the SDLC process
- A multi-tiered Application integration and testing strategy, and implementation
- Control of software documentation and associate changes

- A procedure to measure compliance with software development standards
- Measurement and reporting mechanisms

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Application Quality Assurance.

Application Quality Assurance Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Create and submit a quality management approach to be updated in the Standard and Procedures Manual.	X	
2. Review and approve quality management approach.		X
Build Roles and Responsibilities	**Contractor**	**County**
3. Perform formal technical reviews applied throughout the SDLC process.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
4. Provide QA measurements and reporting.	X	

7.2.10. Database Administration

Database Administration Services are the activities associated with the maintenance and support of production databases. This includes responsibility for managing data, monitoring the database, routine maintenance, database log file reviews, dataset placement, database performance, and data recovery and integrity at a physical level.

The following table identifies the Plan, Build and Operate requirements, roles and responsibilities associated with Database Administration.

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Define Database administration requirements and policies including authorization requirements for End-Users, roles, schemas, etc., and approve Change requests.		X
2. Develop and document in the Standards and Procedures Manual Database Administration procedures that meet requirements and adhere to defined policies.	X	

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
3. Review and approve Database Administration procedures.		X
4. Develop and provide database roadmaps for version releases for planning and Portfolio Management.	X	
Build Roles and Responsibilities	**Contractor**	**County**
5. Provide security administration including managing role and End-User database permissions in accordance with County policies.	X	
6. Perform database restores from export dumps or backups.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
7. Create/refresh development/test/QA databases from production data.	X	
8. Execute authorization Service Requests.	X	
9. Define and provide database creation, configuration, upgrade, patches and refresh requirements.		X
10. Execute database creation, configuration, upgrades, patches and refresh.	X	
11. Execute all database system-level changes (e.g., initialization parameters).	X	
12. Execute all schema changes for all instances.	X	
13. Execute database data definition requirements for Applications (IMAR for tables, triggers, attributes, etc.).	X	
14. Maintain documentation for all database instance parameters and system settings.	X	
15. Maintain consistent database parameters and system settings across all like instances; consistency must be maintained according to established development to QA to production life cycle.	X	
16. Execute database data definitions for Applications and developer schemas.	X	
17. Define and execute database performance and tuning scripts, and keep database running at optimal performance for County's workload.	X	

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
18. Implement and administer appropriate database management tools across all database instances. Performance metrics and historical data must be available for trending and reporting over a minimum of 6 months.	X	
19. Identify and resolve locking conflicts, latch contention, rollback requirements, etc., for all database instances.	X	
20. Provide technical assistance and subject matter expertise to County Application developers and Third-Party support.	X	
21. Provide data dictionary expertise, End-User data assistance, Data Warehouse Metadata definition, data mapping functions.	X	
22. Monitor database and generate automatic Service Desk trouble tickets for Incidents.	X	
23. Patch database software as needed according to established development to QA to production life cycle.	X	
24. Manage database communication software configuration, installation and maintenance.	X	
25. Provide database storage management and cleanup activities.	X	
26. Define database backup schedules, retention periods, levels (i.e., full, incremental or differential).		X
27. Execute County's database backup and recovery policies.	X	
28. Deliver backup and restore activities for support and/or as requested via Service Request.	X	
29. Provide database capacity management and availability management. Examples of activities include failover testing, monitoring, performance planning, etc.	X	
30. Maintain storage allocation, file systems and current usage, file system and capacity management.	X	
31. Provide database installation, de-installation and administration, testing, copying, and security and User management.	X	
32. Provide administrative account support.	X	
33. Provision and de-provision all and any accounts that are authorized to be created, changed or modified.	X	
34. Provide system monitoring and documentation	X	
35. Maintain transactional logs and backup upon set schedule.	X	

Database Adminstration Services: Plan, Build and Operate Roles and Responsibilities		
36. Provide operational support of County's public or private cloud databases.	X	

7.3. Application Development Services

7.3.1. Overview

Application Development Services shall apply to functional changes within the existing Application portfolio and any new Application development activities.

7.3.2. High Level Requirements

7.3.2.1. Contractor shall perform all development and integration activities in alignment with the County IT Strategic Plan and strategic roadmaps.

7.3.2.2. Contractor shall ensure integration with existing data or Applications is scoped and delivered per the requirements.

7.3.2.3. Contractor shall ensure all development activity follows the County's Information Technology standards, guiding principles, architecture bricks and patterns.

7.3.2.4. Contractor shall provide technology assistance and support to the County in planning and standard setting activities.

7.3.2.5. Contractor shall create and maintain accurate and continuous prompt updates to be added to the asset and system documentation.

7.3.2.6. Contractor shall ensure cross Framework integration and communication is conducted for Application development requiring cross Framework integrations.

7.3.2.7. Contractor shall provide Services in accordance with ITIL and CMMI standards to ensure practices result in predictable, repeatable, and successful results.

7.3.2.8. Contractor shall review and comply with all County existing technical standards (e.g., naming, JCL, etc.).

7.3.2.9. Contractor shall provide Application integration and testing to confirm that the individual Application Framework Components work together properly and, as a whole, perform their specified functions.

7.3.2.10. Contractor shall provide integration and testing of Interfaces to other Applications already in production at, or developed by, County or Third-Parties as stated in the applicable requirements documents.

7.3.2.11. Contractor shall provide Application data migration associated with the installation and migration of new or upgraded components to the production environment.

7.3.2.12. Contractor shall provide base training to key County personnel when Contractor develops a new functionality.

7.3.2.13. Contractor shall validate that all the activities necessary to design, develop and implement any development or changes are not only effective and efficient for quality assurance and control but geared toward continuous quality improvement.

7.3.2.14. Contractor shall perform QA Services throughout the entire Software Development Life Cycle (SDLC). QA Services include the following:

- A quality management approach
- Effective software engineering technology (methods and tools)
- Formal technical reviews applied throughout the SDLC process
- A multi-tiered Application integration and testing strategy, and implementation
- Control of software documentation and associate changes
- A procedure to measure compliance with software development standards

- Measurement and reporting mechanisms

7.3.2.15. Contractor shall ensure and meet all requirements to transition from Applications Development into Applications Maintenance and Operations support when placed into production status.

Contractor shall perform the Applications Development Services described in the overview, high-level requirements, descriptions and tables in the sections below, as well as the Applications Common Services described below. The sections directly below describe in more detail the requirements, roles and responsibilities in the Plan, Build and Operate format for each specific section.

Application Development Services: Plan, Build and Operate Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Develop Application architecture and future roadmap.	X	
2. Create and deliver high-level Application solution design document, including architecture, functions, data models, design features, configuration, performance requirements (e.g., security, extensibility, maintainability, scalability, availability, and reliability).	X	
3. Identify requirements for Disaster Recovery and Business Continuity Planning.	X	
4. Identify security requirements, risks or vulnerabilities in any solution provided as part of Applications Development and provide plans to address or mitigate.	X	
5. Develop plan and approach to migrate developed Application to M&O Services, including warranty services (if applicable).	X	
6. Review and approve plan and approach to migrate developed Application to M&O Services.		X
7. Participate in periodic technical and business planning sessions to establish standards, architecture, and project initiatives.	X	
Build Roles and Responsibilities	**Contractor**	**County**
8. Review project scope of work to assess alignment with architecture standards, provide recommendations.	X	
9. Assess impacts and linkages to other Applications.	X	

Application Development Services: Plan, Build and Operate Roles and Responsibilities		
10. Develop detailed solution design documentation, including environment configuration, integration requirements and technical details.	X	
11. Review and approve detailed solution design documentation.	X	
12. Recommend implementation alternative approaches.	X	
13. Review and approve implementation approach.	X	
14. Provide updates to Application architecture documents based on as-built development activities.	X	
15. Provide Budget Estimates upon request by the County.	X	
16. Provide Service Request Project Estimates upon request by the County.	X	
17. Review and approve Service Request Project Estimates.		X
18. Assist with development of business requirements as requested by the County.	X	
19. Assist with development of technical statements of work for Application systems as requested by the County.	X	
20. Review and approve business requirements and Applications technical statements of work.		X
21. Assess capacity, availability, and performance impacts for recommended solutions.	X	
22. Identify and communicate any impacts to the Service Request project cost and schedule estimate.	X	
23. Review and approve revised Service Request project cost and schedule estimate.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
24. Alert County to exceptions in architecture standards.	X	
25. Review and approve architecture standard exceptions.		X
26. Identify and document risks/challenges with recommended solution.	X	
27. Monitor technical trends through independent research, and document and report on products and services with applicability to the County.	X	

Application Development Services: Plan, Build and Operate Roles and Responsibilities		
28. Recommend SDLC process improvements, and document in Standards & Procedures Manual if approved by the County.	X	
29. Support market scans upon request to explore Third-Party solutions.	X	
30. Conduct/coordinate Application evaluations of new products/services.	X	
31. Evaluate and recommend upgrade process for new Application system versions.	X	
32. Develop and communicate risk assessment for development efforts and implementation.	X	
33. Develop project plan, including cost and schedule estimates.	X	
34. Review and approve project plan, including cost and schedule estimates.	X	
35. Develop logical and physical data models.	X	
36. Develop and maintain requirements traceability matrix.	X	
37. Develop prototype Applications to evaluate functionality, requirements.	X	
38. Ensure updates are made to Applications repositories, Configuration Management, and Asset Management.	X	
39. Adhere to Release Management policies/procedures.	X	
40. Develop Application functional requirements documents and conceptual data models.	X	
41. Review and approve functional requirements and conceptual data models.		X

7.4. Electronic Health Records (EHR) Program Management Services

7.4.1. Overview

7.4.1.1. EHR Program Management Services support the use of existing EHR and implementation of additional EHR capabilities to meet operational needs. EHR Program Management Services shall have

a designated EHR Program Manager under the Agreement and will be staffed accordingly.

7.4.1.2. EHR Program Management Services shall be provided to various Health and Human Services Agency (HHSA) programs including but not limited to HHSA Information Technology Services (ITS) and staff and contractors involved in the implementation and/or support of clinical systems in HHSA.

7.4.2 High Level Requirements

7.4.2.1 Contractor shall engage a qualified EHR Program Manager.

7.4.2.2 The EHR Program Manager shall work with HHSA Director, ITS and/or other leader(s) designated by the HHSA Director.

7.4.2.3 The EHR Program Manager shall develop technical program/project management best practices/templates and provide training/mentoring to project teams.

7.4.2.4 The EHR Program Manager shall monitor dependencies across multiple interrelated technical projects.

7.4.2.5 The EHR Program Manager shall gather and report consolidated technical project status and financial information to HHSA leadership.

7.4.2.6 The EHR Program Manager shall assist a central governing body to review/audit adherence to methodologies, budgets, and timing.

7.4.2.7 The EHR Program Manager shall assists HHSA leadership in managing EHR projects/programs.

7.4.2.8 The EHR Program Manager shall oversees short to mid-term (1-3 years) EHR strategy execution and operations in alignment with HHSA objectives.

7.4.2.9 The EHR Program Manager shall provide oversight of multiple concurrent clinical systems projects.

7.4.2.10 The EHR Program Manager shall makes decisions which have a serious impact on the overall success or failure on area of accountability.

7.4.2.11 The EHR Program Manager shall collaborate with project managers and business sponsors to ensure value delivery.

7.4.2.12 The EHR Program Manager shall provide recommendations, performance metrics, and measurements based on HHSA goals.

7.4.2.13 The EHR Program Manager shall monitor project portfolio reporting and provide program-level reporting to stakeholders.

7.4.2.14 The EHR Program Manager shall gather, manage, and prioritize high-level operational requirements to be leveraged in the development of solutions to meet HHSA business needs.

7.4.2.15 The EHR Program Manager shall advise and support HHSA stakeholders on Contractor's processes and standards.

7.4.2.16 The EHR Program Manager shall coordinate work request submissions.

7.4.2.17 The EHR Program Manager shall maintain list of HHSA clinical system projects and priorities.

7.4.2.18 The EHR Program Manager shall perform a monthly program review to include a summary of program management activities, relay HHSA requests, review active project log and status, and identify Contractor support needs for upcoming projects.

END OF SCHEDULE

Appendix 4.3-1 Contractor's Solution

Table of Contents

1. Overview of Services 5

2. Cross Functional Services 8

2.1. Overview 8

2.3. Contract and Acquisition Management Services 8

2.4. Integrated Asset Management Services 11

2.5. Billing Management Services 19

2.6. Security Management Services 22

2.7. Service Delivery Management (SDM) Services 31

2.8. [Reserved] 35

2.9. Project Management Services 35

2.10. Integration and Testing Services 41

2.11. Incident Management Services 47

2.12. Problem Management Services 51

2.13. Change Management Services 54

2.14. Release Management Services 56

2.15. Configuration Management Services 58

2.16. Capacity Planning and Performance Management Services 61

2.17. Disaster Recovery Management Services 65

2.18. Identity Access Management Services 69

2.19. Reporting Management Services 75

2.20. Domain Name Management Services 77

2.21. Business Analyst Services 78

2.22. Chief Technical Architect (CTA) 84

2.23. Enterprise Application Architect (EAA) 89

2.24. Innovation Management Services 90

3. Service Desk Services 93

3.5. Service Request Management Services 106
4. End-User Services 108
4.5. Desktop Computing Services 115
4.6. Core Software Services 125
4.7. County Retained Assets Services 127
4.8. Mobile Device Support Services 128
4.9. Unified Communications Services 132
4.10. Catalog Services 137
4.11. Network Printer Services 139
4.12. [Reserved] 142
5. Network Services 143
5.5. Data Network Services 152
5.6. Remote Access Services 155
5.7. Voice Services 158
5.8. Network Security Services 163
5.9. Video Conferencing Services 165
5.10. Video Streaming and Archiving Services 168
5.11. Mobility Infrastructure Services 169
5.12. Wireless Network Access Services 171
5.13. Third-Party Network Access Services 173
5.14. External DNS Management Services 174
5.15. IP Address Management Services 175
5.16. New Site Installation Services 176
5.17. Interactive Voice Services 178
6. Data Center Services 182
6.5. Security Services 190
6.6. Mainframe Services 193

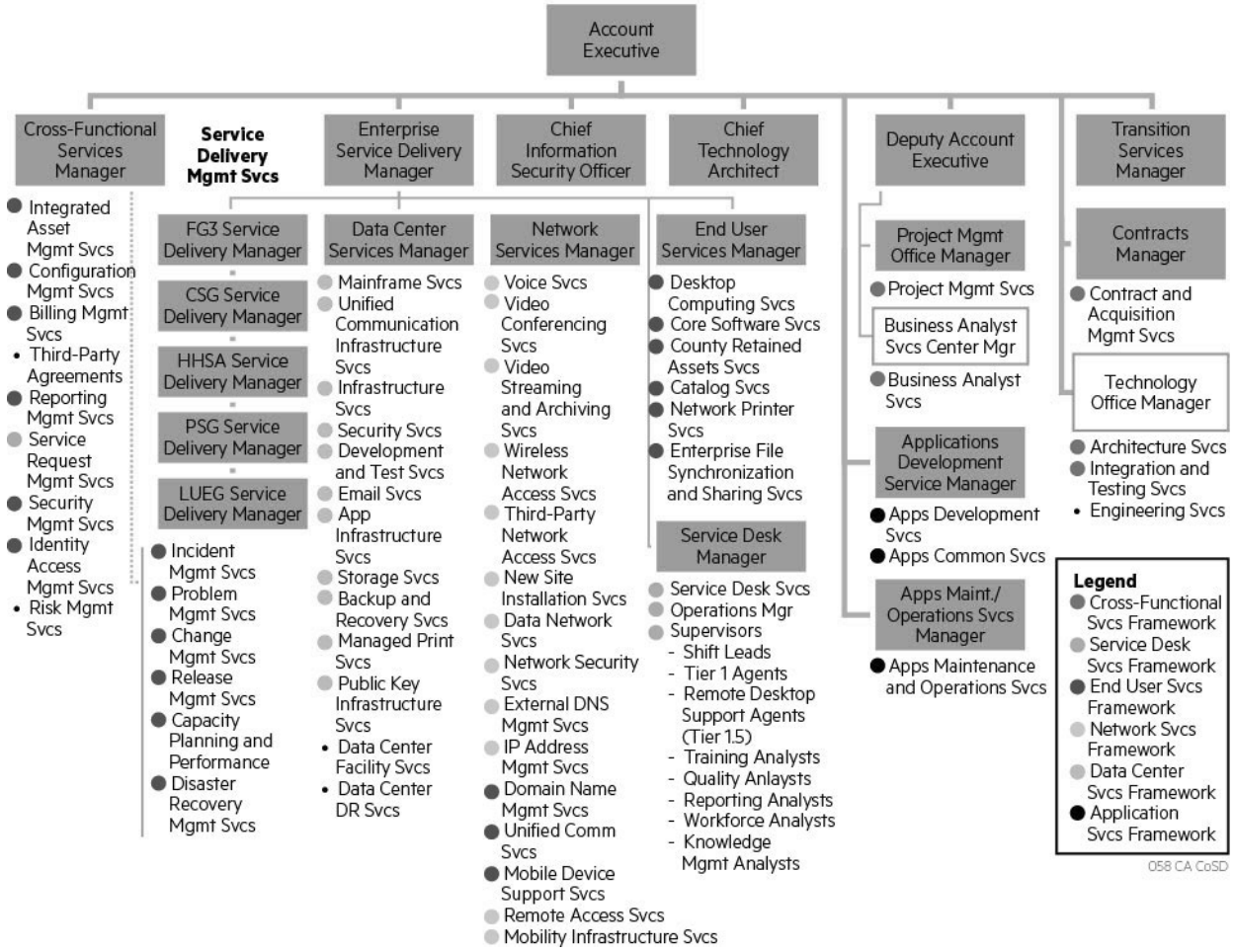
6.7. Application Infrastructure Services 194
6.8. Infrastructure Services 200
6.9. Development and Test Services 205
6.10. E-Mail Services 208
6.11. Unified Communications Infrastructure Services 216
6.12. Storage Services 217
6.13. Backup and Recovery Services 221
6.14. Managed Print Services 227
6.15. Public Key Infrastructure (PKI) Services 229
7. Applications Services 232
7.2. Application Maintenance and Operations Services 232
7.3. Application Development Services 246
8. Transition Services 266
8.1 Transition Services 266
8.2 Transition Project Plan 268
8.3 Transition Staffing 268
9. Transformation Projects 303
9.1. Transformation Services 303
10. Contractor Tools 351
11. County Applications by PA-ID 371

The following sets forth the Contractor's solution for its performance of the Services under this Agreement. Contractor represents that the solutions set forth below are intended to meet many of the requirements of the Agreement. Nothing in this *Contractor Solutions* shall relieve Contractor of its obligation to perform all Services under the Agreement and to perform the Services in accordance with the standards and requirements set forth in the Agreement.

1. OVERVIEW OF SERVICES

1.1.1. Organization and Staffing

The following organization chart shows Contractor's staffing at a role level and the reporting relationships, including Subcontractors, starting from Account Executive and broken down into Service Frameworks.



*The above org chart does not reflect the following positions EAA and Innovation Officer

Centers of Excellence

Geographic deployment of resources at a role level

The Contractor team shall provide services from mainly five (5) locations: County of San Diego; Pontiac, Michigan; Tulsa, Oklahoma, Colorado Springs, Colorado, and El Paso, Texas, with a few individual support

personnel at various sites within the United States (individuals who work from home). These sites shall house staff, equipment, and services needed to respond to inquiries over the telephone and by fax, email, and web-based media including web forms. Contractor shall provide support 24x7x365. The following table lists the percentages of services provided from each location.

Service Frameworks

LOCATION	SERVICE DESK SERVICES	END-USER SERVICES	NETWORK SERVICES	DATA CENTER SERVICES	APPLICATION SERVICES
County of San Diego	20%	100%	80%	10%	75%
Pontiac, MI	80%			5%	5%
El Paso, TX					10%
Tulsa, OK			10%	65%	
Colorado Springs, CO				5%	
Other resources			10%	15%	10%

Project Staff Selection and Replacement

Selection and replacement procedures for the project staff

Contractor's process for selection of personnel to support the County under this Agreement shall be as follows:

- Available positions are announced to the existing team
  - If a current employee is qualified and interested, they may post for the position
- Positions are posted on Contractor's websites and on Smart Buy
- Interested Contractor, third parties, and external candidates may apply
- Normal hiring process includes interviews by the account team to determine technical competency and fit within the account dynamic.

As relates to the County's request to maintain specific staffing assignments:

If a Contractor employee staffing an assignment under this Agreement requests to move to another position within Contractor's organization, the account team shall post the position, identify a suitable replacement, notify the County (if this person is County-facing), and develop a cross-training plan so that the new team member is ready to assume the duties on the outgoing employee, making for a smooth transition. Typically, an employee shall remain in his/her position for a minimum of 2 years before applying for other positions. To apply for open positions prior to the minimum time requirement, approval of the employee's manager is required.

If a Contractor employee staffing an assignment under this Agreement leaves unexpectedly, the account team shall immediately assign a temporary backfill to review in-flight projects and minimize disruption to the County. In parallel, the account team shall post the position, identify a suitable replacement, notify the County (if this person is County-facing), and develop a training plan to make certain that the new team member has the tools necessary to perform the required functions.

Key Positions / Key Personnel

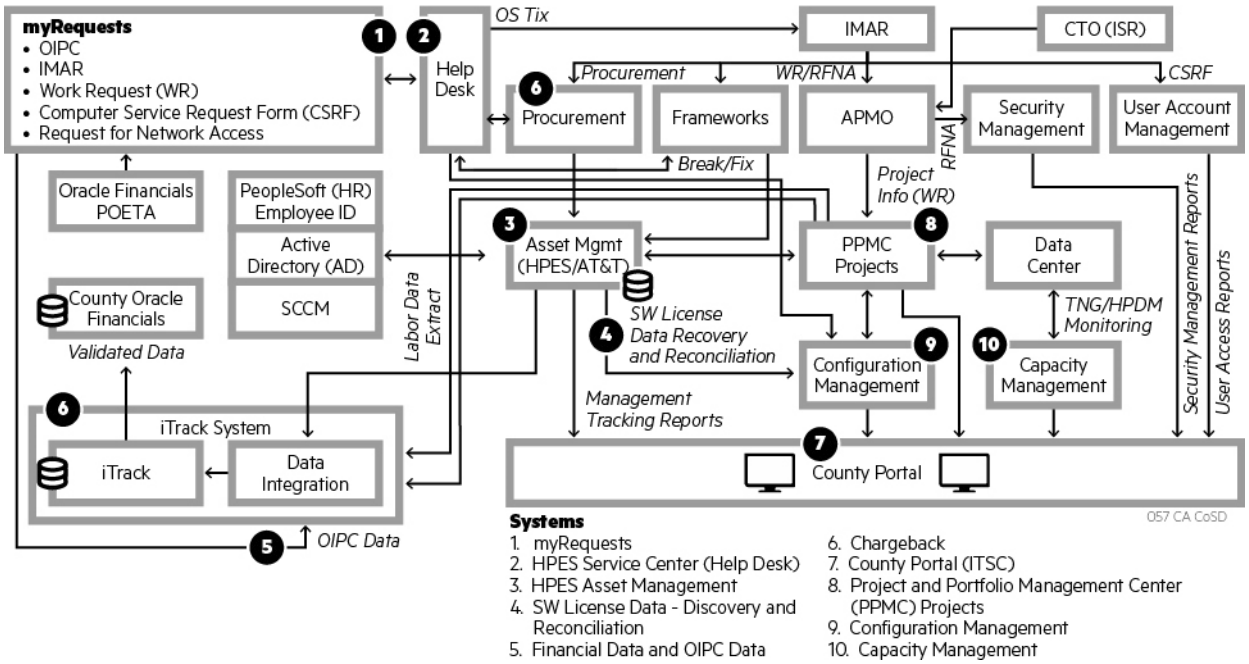
Named Position	Key Positions
Cathy Varner	Account Executive
Laura Floyd	Deputy Account Executive
Kathleen Barghols	Enterprise Service Delivery Manager (SDM)
John Steed	FG3 Service Delivery Manager (SDM)
Frank Krone	CSG Service Delivery Manager (SDM)
Sandra Messina	HHSA Service Delivery Manager (SDM)
Albert Hatcher	PSG Service Delivery Manager (SDM)
David Pugh	LUEG Service Delivery Manager (SDM)
Max Pinna	Contracts Manager
Marcelo Peredo	Chief Information Security Officer (CISO)
Thif Iruthayarajah	Chief Technology Architect (CTA)
Jayaprakash Boreddy	Enterprise Application Architect (EAA)
Mark Morin	Cross Functional Services Manager
Curtis Yancey	Service Desk Manager
Hector Vaquedano	End User Services Manager
Jeff Williams	Network Services Manager
Michael Boscarino	Data Center Services Manager
Tina Terlecki	Application Maintenance and Operations Services Manager
Mark Roehr	Applications Development Services Manager
Nelson Diaz	Project Management Office (PMO) Manager
Chris Spanka	Transition Services Manager
<TBD>	Innovation Officer

2. CROSS FUNCTIONAL SERVICES

2.1. Overview

Contractor shall reliably manage the County's IT environment through a consistent and standardized Cross Functional Services model, illustrated in the figure below.

Contractor Cross-Functional Services Model



Delivering centrally managed, cross-functional uniformity of County cross-functional IT services.

Contractor's Information Technology Infrastructure Library (ITIL)-aligned service management practices shall support all Contractor-delivered IT services, making certain that its service delivery meets or exceeds County requirements and expectations. Contractor shall employ industry best practices, processes, and methodologies, optimally combining people and technology to fulfill the County's IT objectives. Contractor shall coordinate and collaborate with County leadership, limiting or preventing misunderstanding and miscommunication through full and open transparency.

Service Now is also under review as an alternate solution for the Standard Reference Architecture (SRA) stack and its functionality. Details of the specific tool used shall be discussed and documented to prepare a notice of decision (NOD) during Transition planning.

2.3. Contract and Acquisition Management Services

2.3.1. Process and Procedures

Contract and Acquisition Management

- Description of solution to meet the requirements

Solution: The Contractor solution shall include an experienced, full-time contracts manager to serve as the single point of contact for the County on all contractual matters, including subcontracts and third-party vendor relationships. Responsibilities shall encompass all contractual issues between Contractor and the County, including contract interpretation, service requests, estimates and pricing discussions, and contract changes and disputes.

The contracts manager shall establish contractor oversight responsibility and provide recurring status reports to the County contracts manager on contractual matters and shall work with County counterparts to respond to unscheduled requests for information. In addition, the contracts manager shall interact with subcontractors and vendors to audit and verify the timely provision of the requested services.

Contractor's contract management activities shall build performance evaluative criteria to assist the County contracts manager in determining compliance with the Agreement.

- Deployment plan for resources and use of facilities

The Contractor's contracts manager shall oversee the delivery of the contract management services. The contracts manager shall be knowledgeable about the County's business and services. A subcontracts manager, procurement specialists, and Contractor's Global Procurement organization shall provide acquisition management. The contracts manager shall be co-located in the County Technology Office, with a satellite office in Rancho Bernardo.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's methodology shall include performance-based management and includes periodic assessments of Contractor's key performance indicators (KPIs). Contractor shall continually assess these indicators to identify negative trend lines. Contractor shall conduct root cause analysis, where necessary, and take appropriate remediation steps to improve the KPIs and positively influence performance trends—thereby facilitating year-to-year continuous improvement.

Adherence to County procurement policies and procedures when engaging, selecting, and contracting with Third-Parties, including ensuring pricing is fair and reasonable.

Contractor's Global Procurement organization shall be responsible for making certain that all procurements corporate-wide are performed in accordance with all federal, state, and local laws and policies and that goods and services are purchased at fair and reasonable prices. Contractor's procurement team shall maintain active and historical records of trusted and vetted third-party vendors from whom Contractor solicits proposals and/or quotations for County goods and services. Additionally, Contractor shall verify that goods and services provided were delivered in accordance with Agreement requirements and County expectations. Moreover, Contractor's sourcing and procurement team shall flow down all relevant terms and conditions to third parties to verify that all of the County's requirements are met.

Approach for conducting market scans to purchase Assets from Third-Parties.

The Contractor procurement team shall submit requests for quotations (RFQs) to a subset of vendors identified by Global Procurement as best-in-class providers in their database-based Dunn and Bradstreet (D&B) ratings and other factors as a starting point. Contractor shall continually update this database of vendors to provide a large pool of vendors who offer competitively priced goods and services. Contractor shall use the County – Vendor and Product Assessment Process for vendor and product assessment projects requests. Additionally, Contractor's account subject matter experts (SMEs) shall assist in market scans by attending conferences and staying abreast of the latest technologies and products and making the Contractor procurement team aware of them. Contractor's

procurement specialists shall work closely with County personnel to make certain that Contractor captures and understands their needs. Contractor shall routinely follow up with them to verify their ongoing satisfaction.

Management, maintenance and publication of the Optional Item Catalog (OIC).

The Contractor desktop catalog manager shall be responsible for managing, maintaining, and publishing the OIC. Contractor shall publish and manage the OIC via the Contractor Service Portal.

Contractor shall issue quarterly requests for quotation (RFQs) for the entire hardware catalog to multiple top-tier suppliers. Contractor shall publish the lowest price obtained for each item in the OIC. If an item is not available during the 3-month period from the low-price vendor, then Contractor shall notify the County and request permission to purchase at the current price.

End-Users shall place acquisition requests through the Service Portal for acquisition of items from the OIC.

Relationships and existing agreements Contractor has with Third-Party developers of government and commercial software products, and how these can be leveraged and accessed by the County.

Contractor has negotiated master service agreements and strategic alliances with a number of IT and enterprise solution vendors, such as Oracle, EMC, Microsoft, Palo Alto, and so forth. Where these negotiated master service agreements and strategic alliances provide expedited access for technical support specific to the third-party vendor's product or software ("reach-back"), Contractor shall provide reach-forward and reach-back to leverage the Contractor leveraged organization for on demand technical support and services. Contractor shall contract with third-party developers on behalf of the County to use Contractor's volume discounts, terms, and conditions.

Managing the County's Desktop Applications Directory (DAD)

After the review team approves the addition to the OIC Catalog for new Desktop Applications Directory (DAD) software, then the Contractor's desktop catalog manager shall add the software to the OIC Catalog (updates to Service Portal OIC Catalog are posted on the 20th of each month). This shall include purchasing software, verifying County-owned software, and transferring software requests to Desktop Engineering. After this is complete and the software is posted to the OIC, the Contractor's desktop catalog manager shall take the licensing documentation and input the data into Contractor's asset database as new DAD entry(ies) updating the Asset Management Database. To manage the DAD item volume, Contractor shall periodically produce and review with the County a report showing the last order date of all DAD items, as well as the number of instances installed. Contractor shall remove items from the DAD that are no longer being ordered to remain within the DAD limits.

Description of how hand off and touch points are managed to be seamless to the County End-User requesting the Service (e.g., Contract Management Services, Applications M&O Services, Applications Development Services, Service Desk Services, Network Services)

Contractor, in cooperation with County stakeholders, shall maintain policies, procedures, and best practices to enable the seamless provision of IT services as projects or service requests transition from point to point through instantiation or implementation.

When the End-User requests a project, then he or she shall fill out a form with the required fields and a Statement of Work (SOW) describing what he or she is trying to accomplish. After the service request form is finished and approved by the County, then the request shall be sent to Contractor as a request for a Budgetary Estimate (BE). The Contractor PM and technical team shall prepare the BE with scope, requirements, assumptions, and a cost estimate for the requested work. Once approved, the project shall proceed to the scope execution phase. Changes in scope shall be evaluated within the change management review and approval process. After the scope is completed, the project shall be formally closed down. The Contractor PM shall prepare a Project Closure

Agreement (PCA), and the Contractor project support office (PSO) shall send it to the County for approval. If not approved, the Project Closure Agreement shall be sent to the Contractor PM for updates and then returned to CTO Contracts for approval. If approved, the project shall be officially closed, and the data in the PCA shall be legacy data for the project. These Contractor and County tailored policies and best practices shall be continually refined to minimize End-User impact and disruption—enabling seamless implementation of the requested services.

Evaluating security to ensure the County is aware of the risks or issues in cloud-related services to enable the County to make an informed decision based on Contractor recommendations.

To provide adequate evaluation of risks and issues in cloud-related services, Contractor shall follow the County Cloud Service Provider Request procedures, as well as Contractor's Global Procurement organization's cloud service provider review process. The Contractor Global Procurement processes shall include reviews of liability, data protection and security, termination rights, location of services, location of jurisdiction of services, control/visibility of subcontracting, rights to suspend service, and unilateral/provider amendments to service features. Contractor shall develop policies, architectures, and solutions necessary to facilitate confidentiality, integrity, and availability of the County's data and systems. Contractor shall analyze evolving County architectural landscapes along with security and privacy controls, backup and continuity requirements, and user access and permissions. In addition, Contractor shall factor these and other considerations into its cloud recommendations and governance guidance for presentation to the County. Contractor shall apply the right level of logical and physical monitoring and management of County data center operations and cloud-based assets.

Contractor's security experts shall be well versed in cloud selection, migration considerations, and End-User accessibility as well as denial of service to unauthorized or outside sources. Contractor shall closely monitor these operations to facilitate strict security compliance and security risk mitigation.

2.4. Integrated Asset Management Services

2.4.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor shall provide an Integrated Asset Management System (IAMS) that reduces the amount of manual intervention required to verify, check, and fulfill requests while adhering to governing policies and standards.

It is important that Contractor answer five fundamental questions to demonstrate the scope and dimensions of effective asset management:

- What do you have?
- Where is it?
- How well is it working?
- How much does it cost?
- How well does it support your business?

IT asset management (ITAM) shall address these questions by providing processes, tools, data, and people across the entire life cycle. ITAM shall manage the legal obligations associated with vendor warranties and support commitments, entitlements, and asset disposal.

Contractor's solution is based on an upgrade to HPE's Asset Manager from Asset Center. Asset Manager influences IT operations and decision making in the following ways:

- Aligns services to their supporting assets and contracts
- Effectively manages contracts, license agreements, and warranties

- Streamlines the fulfillment of goods and service requests from the service catalog
- Effects complete asset and project audit tracking
- Proactively identifies license compliance issues
- Evaluates opportunities on license maintenance
- Reharvests and reallocates unused software licenses.

As demonstrated in the table below, benefits to the County include productivity, cost control, and risk mitigation.

Benefits Provided to the County

	PRODUCTIVITY	COST CONTROL	RISK MITIGATION
Hardware Asset Management	• Centralizes information and reporting to give the County a "single source of truth." • Organizes required data and provide reporting for compliance with privacy, security, and environmental regulations. Minimizes the risk of noncompliance with software contracts and auditing costs and potential penalties. • Improves asset repository accuracy by highlighting any unauthorized install, move, add, removal (IMAR) to assets.	• Maximizes use of existing hardware assets across the enterprise	
Software Asset Management	• Centralizes information and reporting to give the County a single source of truth.	• Maximizes use of existing software assets across the enterprise • Verifies the number of licenses in use and determines future licensing requirements based on business demands. • Assists in maintaining compliance with license agreements.	• Assists in detecting unauthorized software and enforces software restriction policies relating allowable software that is allowed to run in the County environment.
Hardware Logistics	• Provides reliable system integration facilitating correct configuration and staging of new and replacement devices so that employees are up and running with minimal downtime.		

- Deployment plan for resources and use of facilities

The following resources are required to implement the Contractor solution:

- IT asset manager
- IT SW asset manager

- Warehouse lead
- End-User HW asset analysts
- End-User SW asset analysts
- Server SW asset analysts.

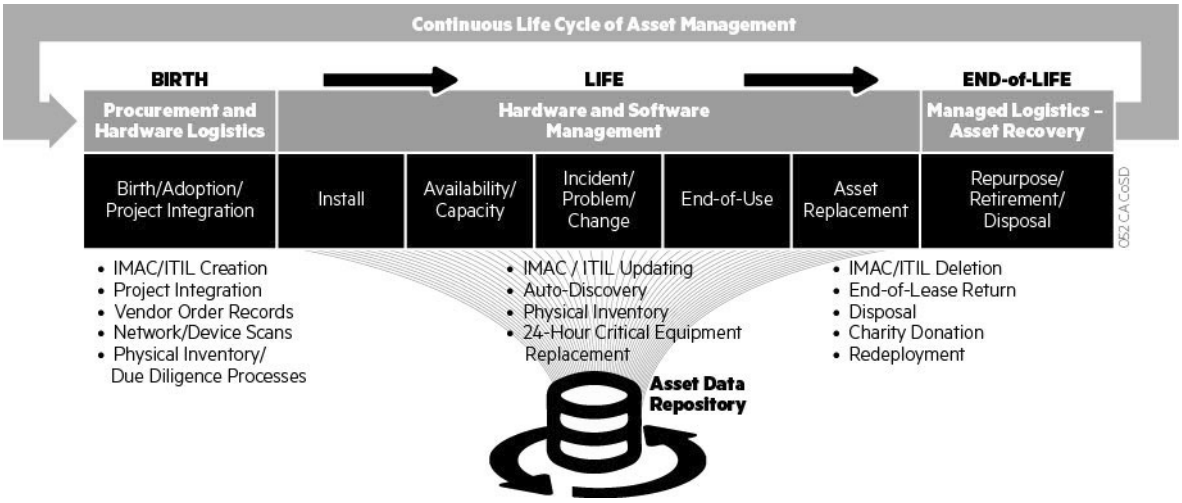
The IT asset manager and warehouse lead shall operate from the Contractor's Rancho Bernardo facility. Contractor shall also leverage resources located at its Tulsa data center the asset management team shall process assets into Asset Manager and provide site support technicians based out of the Rancho Bernardo facility during IMARs, break-fix, and refresh projects for deployed desktop assets.

Contractor shall use a facility approach for stocking the asset inventory, employing two levels of warehouse stocking to speed delivery of equipment in support of IMARs and refresh, while mitigating both inventory and manufacturer disruption risks. County-specific inventory shall be held first at the Contractor's Rancho Bernardo facility and secondly at its partner locations.

- Key methodologies and processes in solution including year-to-year continuous improvement

The Contractor's asset management process shall track all facets of IT assets, from request (procurement) to problems or changes to the asset during its useful life, to disposal (end of life). The life cycle of County asset process is depicted in the figure below.

Contractor Asset Life Cycle Management Process



Providing complete visibility of all County assets throughout their entire life cycle.

Hardware Asset Management

Hardware asset management shall include asset tracking and lease contracts, providing an asset repository that includes records of all hardware assets. Contractor shall track, report on, and analyze the assets from the asset repository.

By tracking assets through the asset repository (database) using various methods and toolsets, Contractor shall capture and report the asset configuration information at the device level (for example, desktop, network, and server). Contractor shall manage the accuracy of the information through cross-checks with other systems and through process links from other services such as Service Desk, site support, and workplace server management services.

The table below identifies the County's high-level deliverables for hardware asset tracking.

High-level Deliverables

DELIVERABLE	ACTION
Asset Repository	• Populates the asset repository with inventory records established during implementation
Asset Record Creation	• Ongoing – as new assets are procured, records are created and added to the asset repository
Asset Tracking	• Updates asset records in repository to reflect the IMAR work process while it takes place • For servers, a discovery tool remotely accesses devices and provides a channel for validating asset records • Reviews and resolves conflicts or exceptions and mediates them in the asset inventory
Reporting	• Creates standard reports documenting the current inventory • Documents inventory asset data elements specified in the table below • Documents data elements for assets that have gone through IMAR or other change processes • Records and reports on listings of noted discontinued hardware
Monthly Evaluation of Asset Accuracy	• Performs audits on approximately 10 percent of the in-scope asset records to confirm continued asset accuracy • Uses various tools to cross-check accuracy of asset data and records
Asset Exceptions Review and Resolution	• Identifies and remediates exceptions

Hardware Lease Contract Tracking

Contractor's lease contract tracking increases awareness of all applicable hardware lease agreements for the hardware assets including desktop, midrange, and mainframe platforms provided as a Service. This service synthesizes basic asset data with information from leasing company sources to enable tracking of all assets under lease and of those that are imminently scheduled for lease expiration.

Maintenance Contract Tracking

Through this service feature, Contractor shall compile data and aggregate it into reports detailing the general contract terms for all Assets covered under warranty, including scheduled contract expirations. From this data, Contractor shall prepare a monthly expiration report highlighting potential renewal or replacement actions.

Contractor shall track maintenance contracts to produce the following benefits:

- Provides a single database for easy access to all warranty and maintenance contracts
- Fully uses warranty and maintenance contracts and avoids expenditures for costly third-party maintenance
- Ensures ongoing warranty and maintenance coverage, where applicable.

Data collected for Warranty and Maintenance Contract Tracking and Lease Tracking is shown in the table below.

Data Collected

FIELD NAME	FIELD DESCRIPTION
End Date	Lease or maintenance contract end date

FIELD NAME	FIELD DESCRIPTION
Expiration Date	Warranty end date
External Reference Number	External reference number (contract number)
Maintenance Contract	Number of maintenance contracts associated with an asset
Purpose	Purpose of contract
Start Date	Contract start date for lease or maintenance

Software Asset Management

Contractor shall provide software asset management to effectively manage, control, and protect the licensed software assets throughout their life cycle. Coverage shall include all in-scope desktop, midrange, and mainframe software that meets registration requirements and has the base data fields required for tracking. This includes both Desktop Applications Directory and Portfolio Applications.

Contractor shall employ standard processes to track and maintain records for:

- Auto-discovered software found during environment scans
- Any transferable details from prior hardware asset tracking discovery
- COTS applications
- Contractor-procured, -owned, and -managed COTS software, as applicable
- County-retained and Contractor-managed COTS software

Software asset management shall include the following services for in-scope software publishers and titles:

- Software license entitlement reporting
- Software installation reporting
- Software license and maintenance tracking
- License compliance management services

Software asset management for desktop and Portfolio Applications shall follow the same high-level lifecycle processes. Creation of the asset record in the IAMS shall occur upon purchase and receipt of the software. The attributes of the assets and associated procurement transactions (ex. vendor, products, license metric, quantity, term, acquisition date) shall be populated in the system and represent the entitlement. Installation records in the IAMS shall be created either through automated discovery or direct entry into the IAMS. Updates to asset records shall be made to reflect IMARs as required.

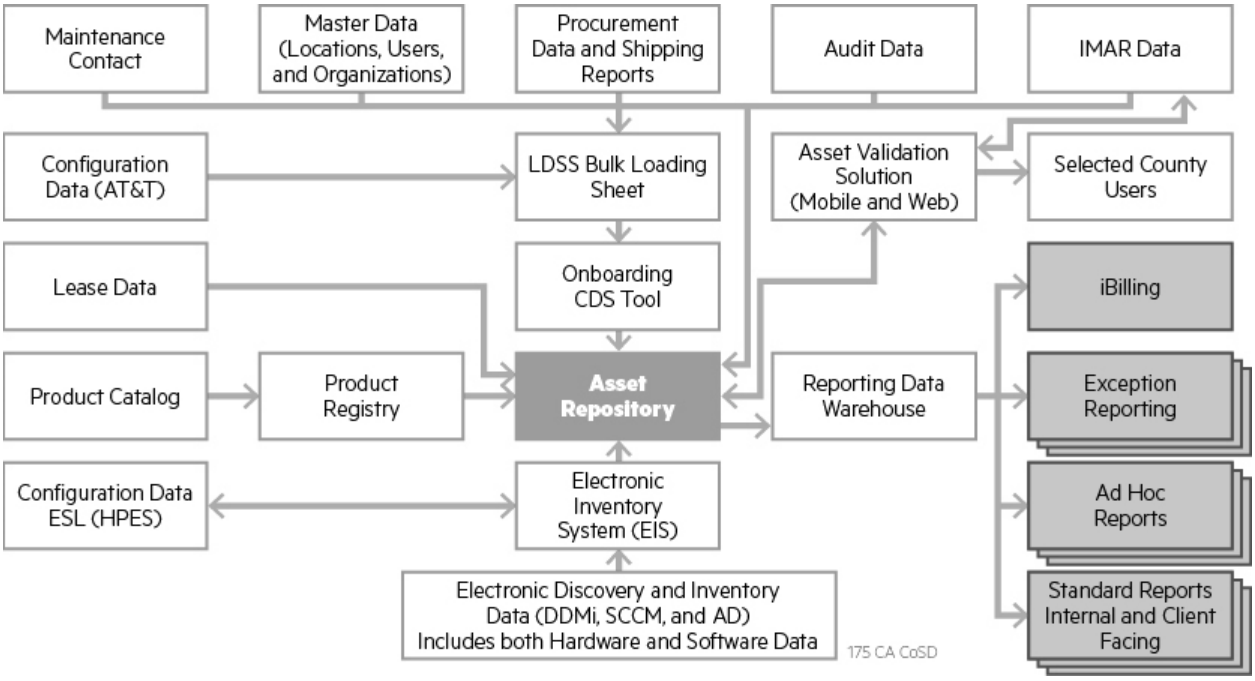
As part of software asset management, Contractor shall maximize use of existing assets through re-harvesting and reallocation of existing software licenses. When there is a requirement for additional software licenses, Contractor shall check whether the current entitlement quantity exceeds the current quantity consumed and, if so, uses the excess licenses to fulfill the requirement. Contractor shall also facilitate workstation/End-User license transfers. Licenses assigned to employees who have left the County shall be reassigned to new hires; also, existing licenses may, from time to time, be reallocated to employees with a current need for that application.

Asset Retirement/Charitable Donation

For retired personal computers, laptop computers, tablets, and associated peripheral assets that were used by the County, Contractor shall donate these assets to the San Diego Futures Foundation (SDFF), at no additional cost to the County.

The figure below depicts Contractor's IAMS. It receives data updates from the Contractor's configuration management database (CMDB), the AT&T CMDB, auto-discovery and inventory tools such as HPE's Discovery and Dependency Mapping Inventory (DDMI), System Center Configuration Manager (SCCM), and Active Directory) as well as bulk load updates and manual updates by asset analysts. Asset data in the IAMS shall be viewable by approved County personnel using the Asset Validation System (AVS) tool, which has a link on the Service Portal.

Contractor Integrated Asset Management System



Automated system to facilitate transparency and accuracy of all software and hardware assets.

Approach to ensure that all Assets Contractor procures for the County are procured in the most cost-effective manner possible, so that the potential reacquisition of such Assets by the County in the event of a disentanglement is favorable to the County.

Contractor's account team shall provide dedicated support from the Contractor's leveraged supply chain practice to source all products and services to ensure Contractor provides the best value for the County. This resource shall be fully aware of Contractor's product needs, shall have leveraged contacts with all Contractor OEM providers, and shall assist Contractor in procuring items in a competitive format.

Contractor shall employ an economic order quantity model to make sure that it is holding the minimum required inventory to be deployed to the County in the case of a disentanglement while still meeting the required refresh and IMAR commitments. This shall include:

- Contractor stocking a supply of desktop and laptop RU hardware units in the Rancho Bernardo warehouse against a 6-month rolling forecast based on the customer-agreed refresh plan and a buffer against IMAR estimates.
- To lessen production disruptions, maintaining agreements with Contractor's value added resellers (VARs) to hold additional supplies of County-specific configured assets in their warehouses.

Integrated Asset Management systems and procedures

The Contractor solution for Integrated Asset Management is based on Contractor's toolset called Standard Reference Architecture (SRA). Integrated Asset Management is a component within SRA. The core software application and repository used for Integrated Asset Management is Asset Manager.

Updates to the SRA toolset shall be made available on a regular basis. Contractor shall conduct reviews of the systems on a semi-annual/annual basis, depending on the tool, to determine whether major upgrades or replacements of systems are required to make certain that Contractor is using the right technology to support the County's needs and remain in supported status.

The primary interfaces into Asset Manager shall include direct use of the client software application, the Load Data Spreadsheet (LDSS) tool for bulk loading of data from spreadsheets, and the Electronic Inventory System (EIS) for electronic discovery data.

The following list contains the Integrated Asset Management systems, data sources, and their integrations:

- **Configuration Data (Contractor)** – ITIL-based Configuration Item (CI) data and Asset Management data shall be integrated. The tool used to manage CI data (ESL) shall be integrated with the tool used for Asset Management data (Asset Manager). Changes in CI data shall be passed to Asset Manager via the EIS system. EIS shall also handle integration of discovery tools including DDMI, SCCM, and Active Directory.
- **Configuration Data (AT&T)** – AT&T configuration data shall be integrated with Asset Manager via the LDSS interface.
- **Product Catalog –**. Contractor shall update the product catalog on a regular basis. It can also be updated with County specific applications. The product catalog shall allow users of Asset Manager to work with a normalized set of asset names.
- **Lease Data** – For those assets that Contractor leases, lease contract data is entered directly into Asset Manager's Contract Module as "lease contracts." Assets are associated with the lease contract under which they were acquired.
- **Maintenance Contracts** – The management of maintenance contracts shall be a standard feature of Asset Manager. Contract data shall be entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool.
- **Master Data –** Master data, such as County locations, shall initially be loaded via the LDSS bulk load tool and maintained on an ongoing basis via the client software application.
- **Procurement Data** – Tracking procurement data for assets shall be a standard feature of Asset Manager. Procurement data shall be entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool upon receipt of the assets.
- **Audit Data –** Tracking audits of assets shall be a standard feature of Asset Manager. Audit data shall be entered either directly into Asset Manager via the client software application or via the LDSS bulk load tool.
- **IMAR Data** – Updating assets in response to IMAR changes (ex. an asset move) shall be performed via the client software application, LDSS bulk load too, or Asset Validation Solution (AVS), described below. AVS shall allow field technicians to directly update Asset Manager in the field.
- **IBilling** – Exports of asset data from Asset Manager shall be imported by the IBilling system for the purposed of billing asset-based Resource Units**.**
- **Reporting** – As part of the SRA toolset, a Reporting data warehouse shall provide support for standard reports, ad hoc reports, and exception reporting.

Contractor's IAMS, described above, shall be accessible to the County. Contractor shall provide a subset of the County manager's direct access to asset manager data using the AVS via the Service Portal. AVS is a web user interface directly reading live asset data.

Ongoing management of the Asset inventory and configuration data.

The Contractor's IAMS shall receive feeds from DDMI (auto-discovery for server) and SCCM and AD (desktop) and be compared to the CMDB and asset repository for accuracy. Asset records shall be updated to reflect that data as necessary, and reports shall be provided to be actioned against when an asset has not been discovered after a set period of time.

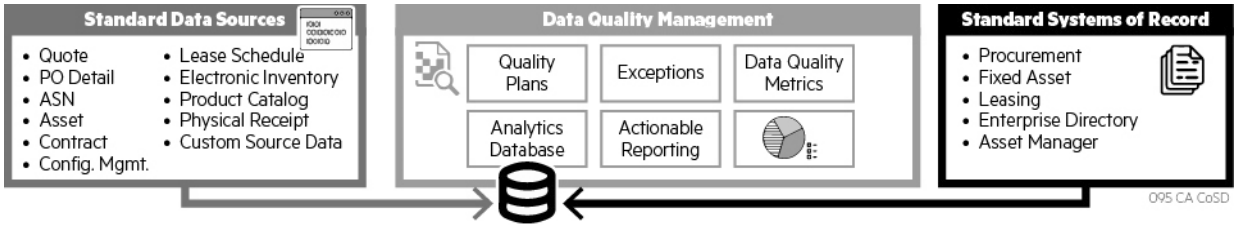
All changes to CI's shall be managed through Contractor's ITIL-based change management process. No changes to assets shall be allowed unless previously approved.

Contractor's CMDB (Enterprise System List - ESL) and Asset Manager shall be housed in a secure, U.S-based network segment on the Contractor's internal network that houses only State and local government data.

Additionally, a comprehensive review of IMAR tickets and refresh project updates shall be undertaken at the beginning of the billing cycle to make sure the asset data is accurately reflected in the files submitted to the iTrack system.

Contractor shall use a data quality management process to validate the accuracy of data in Contractor's database. That process is shown in the figure below.

Data Quality Management Process



Proven process to ensure the integrity of all Asset Management Data.

Contractor shall validate asset accuracy through the following processes:

- Electronic Discovery – validate Asset Manager assets against assets discovered/active as reported in SCCM, DDMI, AD, and SEP.
- Lease Comparison – HP Financial Services asset lease database is compared to Asset Manager.
- Contractor Fixed/Leased Audit – a randomly selected asset sample is validated via auto-discovery or, if required, manual inventory.
- IMAR – Support technicians validate assets when working on machines.
- Onsite Refresh Pre-Field Inspections – desktop and laptop asset data is validated one month prior to a scheduled refresh.
- Contractor Data Center Asset IMACD processes – all parent assets have an affixed RFID tag, which is scanned as the asset enters or leaves the data center floor, updates are passed to ESL, which updates Asset Manager.

Integration of all asset repositories across the Service Frameworks.

The system shall integrate across service frameworks starting with the HPE Asset Manager asset repository containing and receiving updates to:

- Physical servers

- Virtual servers
- Storage frames
- Network appliances
- Discoverable server software
- Desktops
- Laptops
- Workstations
- Tablets
- Network printers
- Discoverable End-User asset software
- AT&T managed network devices

Updates to this data shall be made via bulk loads (for example, refresh projects, move projects, new assets), nightly feeds of Contractor's CMDB data (ESL), AT&T data, auto-discovery and inventory data, and manual updates as requested by service manager tickets submitted to the asset management queue (for example, IMARs).

Integrated reporting across Assets to show useful information relating to departments, hardware, software, licenses, versions, etc.

Deployed and billable server and End-User data shall be pushed to iTrack on a monthly basis. In addition, Contractor shall upload monthly Schedule 5 reports to the Service Portal. These shall include, but are not limited to, the following reports:

- End-User status changes, deployed End-User assets, static access assets report
- Monthly report of installed End-User software titles
- Monthly End-User refresh report

Contractor shall deploy Enterprise Services Asset Analytics (ESAA) data analysis and statistical reporting engine as part of the SRA toolset. This tool shall analyze data stored in Asset Manager and generate standardized reports for analysis and action including the following:

- Asset record completeness (against pre-defined fields)
- Discoverable devices not discovered
- Discovered devices not showing in Active status
- Assets reaching end-of-life
- Devices approaching end-of-lease
- Devices updated in the last month
- Counts of tracked installed software titles versus entitlement counts

Reports shall be provided to the appropriate desktop or server personnel for research, corrective action, and data updates to the source systems if needed.

2.5. Billing Management Services

2.5.1. Process and Procedures

- Description of solution to meet the requirements

The County chargeback application, iTrack, combined with the Contractor billing data consolidation application (IBilling), shall comprise the tools and associated processes for Billing Management.

The iTrack End-User community, County CTO team, and Contractor have identified specific opportunities for incremental improvements. As an example, managing and communicating County low org changes has been a focus area. Contractor is increasing the integration between IBilling and iTrack in support of improved Low Org management by enhancing IBilling to use Low Org data directly from iTrack for data validation. Additional enhancements that Contractor plans to pursue with the County include integration with PeopleSoft HR for employee-related chargeback data and general chargeback data normalization.

- Deployment plan for resources and use of facilities

Contractor shall use the following resources for its billing management services:

- **Billing Manager** – Responsible for the successful delivery of all billing management services
- **Billing Team** – Technical resources to support the IBilling application and the Framework owners responsible for providing monthly billing data and responding to billing disputes.

The billing manager shall be based in the Contractor's Rancho Bernardo facilities.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's methodology shall include performance-based management as well as periodic assessments of Contractor's Key Performance Indicators (KPIs). As an integral component of Contractor's quality assurance management program, Contractor shall continually assess these KPIs to identify negative trends. Contractor shall conduct root-cause analyses where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, facilitating year-over-year continuous improvement.

- Automated systems and tools involved in solution

Contractor shall use the following tools in support of billing management:

- IBilling: Contractor's billing data consolidation application based on SQL Server and SQL Server Integration Services (SSIS).
- iTrack: The County's customized implementation of Nicus' M-PWR commercial off-the-shelf (COTS) chargeback application
- Billing Source Data Tools:
  - AssetManager
  - ServiceManager
  - PPMC
  - Active Directory
  - myRequests (myRequests will be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in Transition Services Framework)
  - AppsManager
  - CSRFs
  - Service Requests

Approach to coordinate and reconcile detailed billings and usage on a monthly basis.

The Contractor billing team shall collect input data from the authoritative source systems by the 5th day of each month for each framework: Application Services, End-User Services, Network Services, Data Center, Cross Functional Services, Special Requirements, Catalog Items, and Other. During this initial data collection phase, framework owners shall review both summary reports and rule-based exception reports to verify data completeness and quality.

Following collection of the framework input data, the data shall be aggregated in a format that can be imported into the County iTrack chargeback system by the IBilling application. IBilling applies rule-based billing logic as

well as data lookup from reference systems. Additional summary, trending, and exception reporting shall be performed on the aggregated data.

By the 9th of each month, Contractor shall review a summary invoice with the framework owners, billing team, and account management. Contractor shall explain any variances and, if needed, make corrections in the billing system and rerun the processes.

After Contractor management approval, Contractor shall create an invoice in Excel— "Base Services Invoice"— and deliver it to the CTO and the office of Auditor and Controller (A&C) no later than the 10th of the month.

Interface of Contractor billing system to County iTrack, and billing data transfer the County iTrack

By the 10th of each month, Contractor shall load detailed billing data into iTrack from IBilling, the Contractor billing data consolidation application, using automated Structured Query Language (SQL) scripts.

County staff shall process the data using iTrack and notify their staff that the data is ready for their review. Contractor shall load detailed telecommunication records by the 10th of the month. Contractor shall archive all billing data, including source files, for audit purposes.

Processes to ensure a high level of billing accuracy each month.

The Contractor billing team and framework owners shall research and address anomalies in trending and exceptions to facilitate a closed loop feedback review and continuous improvement. Contractor shall maintain monthly metrics to track responsiveness to County change requests; Contractor shall monitor and remediate these when necessary as part of its ongoing performance-based management methodology.

Billing corrections

The Change Request process in iTrack shall be used to make billing corrections. The County has until the 22nd of each month to create a Change Request in iTrack to dispute a charge or to request a name, location, low org, or other change to a billing record. On the 23rd of each month, the Contractor billing manager shall generate a report from iTrack of all approved Change Requests for that period and shall distribute it to all framework owners. The Contractor billing team shall investigate, correct, adjust, or explain all disputes and corrections by the next billing cycle. Contractor shall make corrections in the source systems to provide accuracy in subsequent billing periods.

Credits and adjustments for disputed charges, once validated, shall appear as a credit in the next billing period.

Contractor's billing manager shall enter comments in iTrack stating the resolution of each dispute. Contractor shall monitor and follow up on unresolved disputes and track them through closure.

After each billing period, by the 15th of the month, the Contractor billing manager shall compare the Change Requests approved to the latest billing file and shall follow up with framework owners on any differences to verify chargeback billing accuracy.

2.6. Security Management Services

2.6.1. Process and Procedures

- Description of solution to meet the requirements

Contractor's security management shall be comprised of a set of policies and procedures for systematically and quickly reacting to incidents or events that affect the County's information infrastructure, systems, and sensitive data. Contractor shall minimize risk and facilitate continuity of County IT operations by proactively preventing and limiting the impact of security breaches, whether internal or external. Using its expertise and experience, Contractor shall work closely with security counterparts and stakeholders to effectively and efficiently improve County information security. Contractor's solution includes multiple factors that at a minimum include:

- Chief Information Security Officer (CISO)
- Risk management program (framework)
- Evaluation and recommendation for tech controls
- Security governance program/board
- Security and risk management awareness training program
- System categorization for information ownership, classification, accountability and protection
- Incident/threat management and response plan
- Security Information and Event Management (SIEM)
- Continuous improvement

Solution: Contractor's approach to security management shall adhere to the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) and its Special Publication 800 series, which shall act as a guide for delivery and compliance for the protection of systems and providing security services to the County. Overseen by the Contractor CISO, Contractor shall leverage this guidance to methodically assess systems and the organization for gaps and vulnerabilities based on the threat landscape, which may pose a level of risk to the organization.

Contractor shall also use a second approach that coexists with NIST standards, the NSA defense-in-depth model, which emphasizes the use of layers and multiple defense mechanisms across the infrastructure to protect data, systems, networks, and users. In the event that one defensive measure is attacked and exploited, there are additional layers and measures protect the assets.

Additionally, Contractor uses Gartner's Security Process Maturity Model to assess and report the "State of Security" and the progress of various security efforts that contribute to the overall security posture of the County. This model scores areas of security based on scale of 1 to 5 scale—the larger the number, the more mature the security aspect being modeled. Gartner provides a score for "peer" values derived from organizations with similar profiles. This maturity model is useful for comparison over time on how well the County is doing in relation to its peers. Moreover, it provides actionable intelligence for use in Contractor's continuous improvement practices.

The Contractor CISO shall have overall responsibility for all aspects of security (with County CISO). In support of Contractor CISO initiatives, strategies, roadmaps, and transformation, the Security Operations Manager shall be responsible for day-to-day operations and activities.

The following are descriptions of each role and their areas of responsibility:

- IS Security Manager – Responsible for all aspects of compliance, applications security reviews, overall information systems (IS) security, data classification, NIST-based guidance, continuous monitoring of controls, and Security Awareness and Training.

- Security Architect – Responsible for security infrastructure and product roadmaps, strategic participation with other frameworks, establishment of secure zones, and infrastructure security.
- Risk Assessor – Responsible for IS risk assessments, strategic risk guidance, compliance support, vulnerability management support, and vulnerability mitigation support.
- Identity Manager/Analyst – Identity and access management, maintain federated identities, monitors and maintains automated access request workflows, End-User provisioning coordination, monthly IAM reports, yearly attestation process, annual update of IAM plan.
- PKI Administrator – Responsible for use case development in coordination with Security Architect, public key infrastructure (PKI) services delivery, facilitate upkeep of CPS document, manage certificate lifecycle, monthly reporting, PKI inventory, and maintenance of public key certificates.
- Vulnerability Manager – Responsible for continuous scan of the perimeter, vulnerability and risk assessment support, vulnerability mitigation, threat management plan/remediation, application scans, coordinate security operations center (SOC) activities, event log analysis and reporting, intrusion detection system/intrusion prevention system (IDS/IPS) management, data loss prevention support, incident management plan/response/handling, and forensic activities. In the event of a data breach, Contractor shall engage the Security Incident Response Team (SIRT) as necessary to assist in the investigation. This team, in collaboration with the Contractor CISO, shall use its experience and SOC capabilities to ensure that all existing information that aid during a forensic investigation is readily available to authorized individuals. This information shall include log files, SIEM activity, data files, and anything else that may be considered digital evidence. Handling such information must follow proper procedures such as chain of custody and preserving evidence.
- Leveraged SOC – Event log monitoring, single pane of glass, unified threat management, incident response, and IDS/IPS monitoring and analysis.
- AT&T Security – Responsible for providing protection from unauthorized use, access, physical access to County hardware/software (HW/SW), firewall management, event logging, analysis, reporting, IDS/IPS in the communications infrastructure, hardware maintenance, identify and correct single point of failures, architecture and management services, roadmap maintenance for network security services, incident response, data loss prevention support, web content filtering, and hardware maintenance to maximize performance.
- IS Security Officer – Responsible for overall security posture of applications, coordination with application owners, and security documentation.
- HPE Leveraged Services – Forensic services, IDS/IPS service, antivirus services, SIEM services, firewall rule implementation, and PKI support.

- Deployment plan for resources and use of facilities

The Contractor security team shall use multiple locations in support of this Agreement. This team shall work closely with the County CISO, CIO, CTO, and other IT personnel, enabling direct communication and the ability to reach out directly to the Contractor team at any time.

The HPE Rancho Bernardo facility shall be the center of support for Contractor staff assigned to support the County. This facility shall provide centralized meeting spaces for engagements between the County contractors and Contractor personnel. It shall also include test environments, training room, video conferencing, and Contractor executive offices.

HPE Tulsa Data Center shall provide the majority of County IT infrastructure and core IT services, including web, application, DB servers, data storage, and data management.

HPE Orlando data center shall host the leveraged ArcSight SIEM solution from which the county's IT infrastructure is monitored 24x7x365.

HPE Colorado Springs Data Center shall serve as the disaster recovery site for the County IT services.

HPE U.S. Public Sector (USPS) headquarters in Herndon, VA shall serve as the primary location for senior Contractor executives and the Enterprise Security Operations Center (ESOC), a service that monitors the SIEM service.

- Key methodologies and processes in proposed solution including year-to-year continuous improvement

Contractor shall use the NIST CSRC information security tools, practices, standards and guidelines to support the County. The CSRC is the primary source of information for security related standard publications that provide computer/cyber information guidelines, recommendations, and reference materials. In addition, Contractor shall rely on NIST Special Publication 800-53 and 800-37, focusing on the Risk Management Framework (RMF) and the County implementation. The RMF is currently in use by all Federal agencies to comply with FISMA requirements. Contractor understands that the County currently does not have a Federal mandate to comply with FISMA. However, there are some systems in the law enforcement community and healthcare systems that require a proven standard to protect those Federal systems as well as systems that may have interfaces to them. Following is a high-level description of each methodology and key processes that are relevant to the County.

Risk Management Framework – RMF shall be the framework for the County's risk management program and shall provide a standard to measure systems critical to the ever-changing threat landscape in today's County IT infrastructure and systems future hybrid cloud environments. Measuring security controls against an established standard enables best-case resource use and an optimal security posture in which the discovery of vulnerabilities and the time it takes to mitigate them takes as little time as practicable. By following and adhering to the RMF, Contractor is able to minimize potential security oriented exploitation and reduce the risk/impact to the County. The RMF implementation shall continuously look for ways to automate and benefit from technology throughout the duration of the Agreement. The essence of the RMF is its simplicity and its versatility to align and integrate with other frameworks. It employs data visualization technology using dashboards influenced by users and graphical representations to reduce the complexity and improve the accuracy of reporting. The risk-based approach to security control selection and testing provides effective and efficient applicability to the laws and regulations that the County must follow. The steps in the RMF Model are:

- **Step 1: Categorize -** Categorize the information system for ownership, classification, accountability, impact analysis and protection; information is processed, stored, and transmitted by that system.
- **Step 2: Select -** Select an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on the County's assessment of risk and local conditions.
- **Step 3: Implement -** Implement the security controls and document how the controls are deployed within the information system and environment of operation.
- **Step 4: Assess -** Assess the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly and operating as intended, to meet the security requirements for the enterprise.
- **Step 5: Authorize -** Authorize information system operation based on the risk to the County's operations and assets, individuals, third-party vendors; the County determines acceptable risk.
- **Step 6: Monitor -** Monitor and evaluate selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate County officials such as the CISO, CIO, and CTA.

The Contractor security services team shall provide the requisite knowledge and understanding of each control to take advantage of the expanded set of security and privacy controls. This facilitates integration with other frameworks and other County groups that may be considering the implementation of cloud-based solutions with other vendors. In addition to managing complexity, the Contractor security team shall leverage the concept of

common controls and control inheritance to optimally secure each system in the environment. This results in streamlined operations, testing, and more robust application security in already existing traditional and forthcoming cloud hybrid environments.

The tailored RMF roadmap shall make sure that its transition and evolution is low risk, non-disruptive, adaptive, and flexible to meet County demands, as the adoption of cloud-based and hybrid solutions continue to evolve. Security and the RMF are integral to any new IT initiative and avoid the stigma of "delaying" or "preventing" IT projects from moving forward by making sure every stakeholder is informed, educated, and understands the broader and bigger goal of building IT solutions faster and more secure where all frameworks have win-win paths forward.

As more hybrid cloud-based solutions are introduced to solve business needs, Contractor shall rigorously test and enhance the controls surrounding third-party vendors to minimize risk and avoid delays. Controls designed to monitor ingress and egress of data, data flows, audit and accountability, security monitoring, and many others shall be the focus of Contractor when interacting with third-party vendors.

Defense-in-depth –Contractor shall implement the defense-in-depth approach to goal of delaying the attack and buying time to detect and respond in an effort to mitigate or eliminate the consequences of a breach. Elements of defense-in-depth include antivirus, identity management, biometrics, demilitarized zones, data centric security measures, encryption for data at rest and in transit, firewalls, hashing of passwords, intrusion detection systems, logging of events for auditing, multifactor authentication, vulnerability scanning, physical security, access controls, awareness and training, virtual private networks, sandboxing, intrusion prevention systems, and others.

IT Maturity Model – Contractor and the County use a Gartner IT maturity model that assesses the County's information security program and helps provide recommendations for areas of improvement based on the areas identified. It also provides recommendations, technical and non-technical, to address issues. The results shall be presented to the CIO on a monthly basis or as required.

The security roadmap areas of focus shall include but not be limited to:

- **Governance, Organization and Personnel***:* How the County's information security function is organized and governed, and what the scope of the information security program is. How the County staff organizes its information security function, where it gets support from within, where it is supplemented using third-party service providers, and what areas require investment in training and hiring.
- **Policies, Standards, Procedures and Documentation:** How the County articulates and communicates its policies for information security to the business, and how these policies are supported by clearly defined standards and operational procedures. How the County stores and manages the documentation relevant to its information security environment, including as-is state, in-flight projects, assessments, audit findings, and other related materials.
- **Information Classification:** How the County classifies information and critical systems to determine appropriate information security measures based on the organization's appetite for risk.
- **IT Risk Management and Compliance:** Describes the County's risk posture, and how it assesses whether to accept, transfer, mitigate, or avoid certain risks. How the County manages its responsibilities with respect to legal, regulatory, and audit compliance.
- **Identity Management:** How identity management technologies and processes are used to create and manage identities of the various County constituents (e.g., employees, vendors, contractors, etc.)
- **Runtime Access Control:** Determines what technologies and processes are used to manage permissions and access to the County's networks and applications.
- **Software Development and Testing:** Describes how a security mind-set is integrated with software development life cycles, secure coding practices, outsourced software development, and infrastructure deployments. Describes how systematic testing of code, applications, and infrastructure components is integrated in life cycle processes.

- **Applications and Information Repositories:** How security implications relevant to applications, application development, portals, communication and collaboration platforms, file storage and transfer are reviewed.
- **Encryption:** Describes how the County uses encryption for protecting data in transit, data at rest, strong authentication, and digital signing?
- **Security Awareness and Training***:* How the County communicates the importance of information security to the business at large.
- **Change and Release Management:** How the County controls changes in their hardware, software, and supporting infrastructure while maintaining suitable and appropriate information assurance.
- **Incident Response:** How the County responds and escalates responses during critical security incidents.
- **Threat Response:** How the County responds and escalates responses during critical security threats.
- **Resilience Processes:** How the County implements business continuity management and IT disaster recovery planning and testing to protect the resiliency of its infrastructure.
- **Audit Processes:** How regular internal and external audits verify compliance with corporate policies, standards, and procedures.
- **Network Perimeters and Zones:** Determines what network perimeter mechanisms are used by the County to enforce zone boundaries and protect sites, systems, and users across a distributed infrastructure. How zones of trust used by the County to protect their IT resources on communications networks. How the County detects and responds to security incidents on their network.
- **System Zone Placement:** How the County places systems in security zones.
- **Endpoint Admission:** What approaches the County uses to control client endpoint admission to zones and resources.
- **Host Security:** What management and protection postures the County takes with regard to host system security.
- **Vulnerability and Patch Management:** How the County manages and remediates data, software and configuration vulnerabilities.
- **Anti-Malware:** What mechanisms and approaches the County uses to mitigate malicious software such as viruses, spyware, and Trojan horses.
- **Data Loss Prevention:** What approaches the County uses to prevent the unauthorized exfiltration of company confidential information.
- **Security Information and Event Management:** How the County monitors the network and critical systems, including audits of critical system access and logs.

Methodology to protect the security and confidentiality of data and information that is proprietary to the County or subject to special statutory protection

Contractor shall maintain a robust flexible set of risk-based security methodologies to protect the County's information systems and assets. Contractor shall use the NIST RMF, Defense-in-depth, and the Gartner's IT Maturity Model. Additional guiding principles shall include the minimization of the use, collection, and data protection of what is strictly necessary to accomplish county's business. Contractor shall support the County-classified data each system is processing or storing and appropriately determine the levels of protection based on the data classification and impact to the County. Contractor shall then implement the appropriate levels of safeguards based on the data classification. Additionally, a robust set of processes and procedures shall be in place to handle incidents involving the compromise of the data.

The NIST-based RMF fundamental tenets of security include controls that are specifically designed to protect the confidentiality and integrity of data. At a high level, the controls include the creation of policies and procedures, awareness and training, conducting Privacy Impact Assessments (PIA), identifying and classifying sensitive information, and record retention and disposal of information. Other control specifics include:

- **Access Enforcement** – The County controls access to confidential data through access control policies and access enforcement mechanisms. At the enterprise level, employees are part of role-based Active Directory (AD) groups which are determined using a Change Services Registration Form with approval and consent of a

direct employee supervisor. Other non-enterprise systems control access with local management capabilities. As part of the roadmap, a full enterprise identity management capability shall be in place to better secure and manage access controls.

- **Least Privilege** – Contractor shall enforce the most restrictive set of rights and privileges for each End-User in a specific role. For confidential information, Contractor makes sure that users only have access to the minimum about of data needed to perform their job.
- **Auditable Events** – Contractor shall monitor events of systems that contain confidential information and shall make sure there are regular reviews and analysis of system records that indicate inappropriate or unusual activity affecting this data. Investigations shall occur when suspicious activity is detected and violations are reported.
- **Identification and Authentication** – County users shall be uniquely identified and authenticated before accessing confidential information.
- **Media Access** – Contractor shall restrict access to media containing confidential information, often through encryption. Media includes CDs, USB flash drives, backup tapes as well as non-digital media such as paper.
- **Media Transport** – Contractor shall protect digital and non-digital media including confidential data transported outside the organization. A data transfer request process shall be used to scrutinize the data (often encrypted) that leaves County premises.

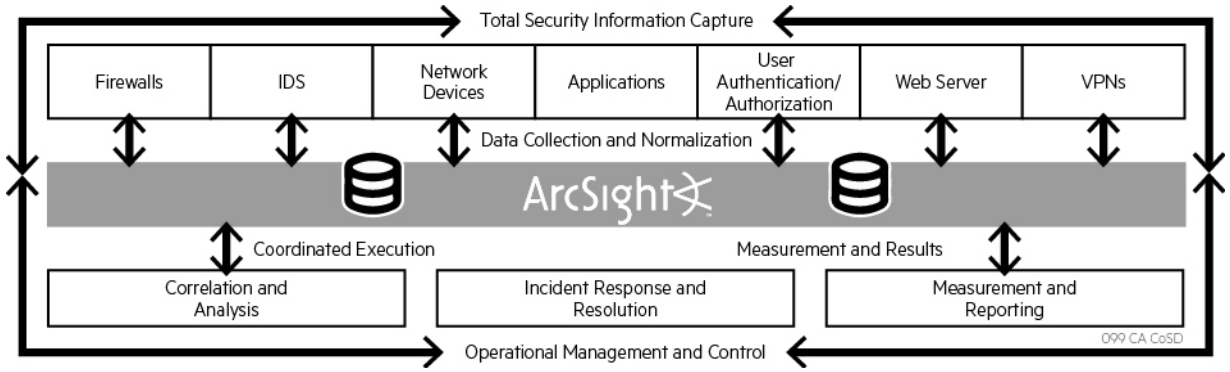
All of these sets of controls shall be implemented at the infrastructure level and on applications that process confidential information. The visibility of how effective controls are being on the lookout for new threats, identifying vulnerabilities, and having a sound mitigation strategy to eliminate or minimize risk results in an optimally protected enterprise.

Approach to data analysis of SIEM information and remediation of identified risks or vulnerabilities.

The major components that comprise the Contractor's SIEM solution shall be: monitored endpoints that generate security events, security data collection servers that collect and normalize events from disparate endpoints, a security information event manager backend that correlates and analyzes collected events and a web portal that presents processed events and alerts. Finally, the SIEM solution shall include security incident response processes to coordinate analysis and resolution of security issues.

Contractor shall use the ArcSight platform, illustrated in the figure below, to perform the aggregation and correlation of security events generated by different data collection points. Palo Alto logging (traffic, threat, and URL) shall be collected by the Palo Alto centralized managed server platform, Panorama. All SSLVPN logging, as well as DHCP logs shall be gathered by the Juniper JSA device. These two devices shall then forward their logs to both the Contractor's SIEM (ArcSight) collector, as well as the AT&T managed SOC group. Data center logging (IPS sensors and firewalls) shall also feed to the Contractor SIEM. Contractor shall analyze and resolve issues to provide an additional layer of security. An event alert from either group shall trigger a collective investigation effort between Contractor and AT&T.

ArcSight Platform



The ArcSight Platform provides tool information security capture, coordination, management, and reporting

At a high level, the process to escalate and respond incidents shall be as follows:

- The Contractor security team shall investigate alerts, determine criticality and, if the criticality is severity one or severity two, shall notify the County and Contractor security about the event. If the event does not meet critical criteria, HPEs shall follow the Contractor's internal procedure for noncritical incidents and shall report to the County in the monthly security reports.
- In the event of a severity one or two, Contractor shall initiate the investigation and contact the County CISO and Contractor operations or any support team requested to alert them of the incident per the Severity Escalation Matrix.
- Contractor shall investigate the incident and activate an incident response team (IRT) as needed. If the documented preapproved, incident containment strategy exists to mitigate threat, the IRT shall immediately execute plans to resolve incident.
- The IRT shall determine resolution strategies for County approval. If required, the team shall initiate the change management process by submitting requests for change (RFC).
- The IRT shall execute a containment strategy upon approval of an RFC, if required. The strategy shall include plans for the prevention of further damage caused by the incident and shall be reviewed by the County CISO.
- The IRT shall execute eradication strategies when the RFC is approved and reported to the County CISO.
- The IRT shall execute recovery strategies upon approval of RFC by the County CISO.
- Contractor shall document the incident and close the incident.
- Contractor shall conduct a lessons learned meeting to update strategies, as needed.

Each process of the SIEM incident response shall be included in the yearly review process, which contributes to the maturity of security services. Any areas of improvement or lessons learned shall be incorporated in the updated process and teams shall be aligned accordingly.

Approach to assess the County's security environment.

Contractor shall continuously monitor in real-time mail threats, inbound and outbound network traffic, and discrete data formats in which information leaves County's networks. Additionally, Contractor's ESOC shall respond to any possible threat by investigating whether it is a true incident or if it is a false positive. False positives shall be used to constantly fine tune IPS/IDS and the heuristic engine for data analysis.

Contractor shall conduct vulnerability scans for a maximum of 3,000 IP addresses in the Front DMZ zone as well as the library network. The plan is to increase the number of servers to include all critical servers based on function and data classification they store or process.

Additionally, Contractor shall conduct scans of servers before they go into production, which results in identification of vulnerabilities in servers before they go live. Contractor shall mitigate high and moderate vulnerabilities before any server goes into the production environment.

Contractor shall conduct policy compliance scans on all production servers on a monthly basis. Contractor shall make sure County servers are compliant with Contractor security policies and are up-to-date with patches.

Contractor shall also execute an annual network penetration test restricted to the DMZ. The Contractor network penetration testing process shall include actions that reduce the risk of exposure to the County's most critical online assets and, detailed descriptions for quickly managing or eliminating security exposures. This streamlined, granular approach to risk management enables security policy compliance to become an integral part of the overall security process.

As part of the RMF, Contractor shall document and test environment controls on a predefined efficient schedule. Contractor shall assess the security controls using appropriate procedures to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the County. The ongoing monitoring of security controls in the environment shall also include documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate County officials such as the CISO, CIO, and CTA.

Contractor and the County CISO shall conduct monthly self-assessment using Gartner's IT Maturity Model and report to the County via CIO briefings. This provides independent validation to the County of Contractor's performance.

Approach to assess the County's application vulnerabilities and security risks, and approach for analyzing and assigning classifications to County Data.

Checklist Based Approach

Contractor shall use an application checklist to identify areas in which the application under review is not compliant with specific security requirements. The application checklist shall be a documented set of questions based on County security policies. The requirements on which the application checklist shall be based are documented in the County Security Management Plan.

The compliance questions shall be categorized into the following security areas:

- Authentication
- Audit
- Nonrepudiation
- Host security
- Enclave
- Access Control
- Confidentiality
- Physical Security
- Application Security
- NIST
- Support
- Integrity
- Network Security
- Data security

Application team members shall respond to an extensive set of questions at different stages of the project, and the list shall then be reviewed by the security team. A scorecard shall then be derived from the questionnaire that

shall be rolled up to a dashboard for all applications going through this process. The dashboard facilities identifying trends within specific security categories across multiple applications.

RMF-Based Approach

Applications shall go through the RMF, as described at the beginning of this section. All applicable controls shall be determined by the data classification and take into account factors such as compliance with HIPAA, Privacy, PCI, and other applicable laws and regulations.

Encryption Requirements for Data Security and Protection

Contractor shall provide the following encryption to protect data in transit, at rest, and the PKI Enterprise implementation:

- Data in transit
  - Transport Layer Security (TLS) – Web servers use TLS with digital certificates provided by Entrust.
  - Secure Sockets Layer (SSL) – Web servers use SSL with digital certifications provided by Entrust.
  - Server Message Block (SMB) – Applied to Windows shares (NAS) and files in transit.
  - Virtual Private Networks (VPN) – Junos VPN uses IPsec tunnel. Traffic between the two points is encrypted.
  - Wireless Encryption – Wireless Access Protocol provides encryption on all wireless data exchanges.
  - Email Encryption – TLS to all inbound connections and to trusted outbound domains. Cisco IronPort Office message encryption.to be replaced with Exchange Online Protection (EOP)
  - Mobile Devices – SSL encryption for all communications with County network when using Pulse VPN. Email is encrypted using TLS inbound and outbound when accepted by both parties.

- Data at rest
  - Endpoint Encryption – Symantec Endpoint Encryption provides maximum protection by encrypting each hard drive sector by sector.
  - Database Encryption – Transparent Data Encryption is used in some SQL databases.
  - Removable Media Encryption – Thumb drives ordered from the catalog use AES 256-bit encryption.
  - Password Hashing – New applications or modified during refreshes that store passwords use hashing algorithms to prevent storage in clear text.
  - Mobile Devices – Devices are encrypted using the Operating System default encryption capabilities where appropriate. Additionally, devices shall use a digital certificate to authenticate to AirWatch.

- PKI
  - User Authentication – Symantec Digital Certificates in Active Directory.
  - Device Authentication – Symantec Digital Certificates in all devices.
  - Digital Signature – Self Signed Digital Certificates by ARX and CoSign.
  - Other use cases shall leverage the current Enterprise PKI Symantec solution.

Contractor shall continue to implement solutions with encryption where technology allows for it. Opportunities to improve in this area include technical refreshes and new implementations.

2.7. Service Delivery Management (SDM) Services

2.7.1. Process and Procedures

- Description of solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

The Contractor approach shall include repeatable, ITIL compliant, delivery of County IT services that consistently provide high-quality IT service delivery across all frameworks.

Contractor's Service Delivery Management services shall be applied and enforced by its enterprise service delivery manager (ESDM) along with the individual service delivery managers (SDMs) assigned per business group. Contractor shall continue its delivery of these services through proactive communication and collaboration with all affected stakeholders. In addition, Contractor shall provide timely guidance and measure results accordingly as required. Contractor shall document its efforts and make this documentation available on the Service Portal. Contractor shall routinely solicit County and End-User feedback as input into its continuous improvement processes.

Solution: Contractor shall assign a single service delivery manager (SDM) to be the point person for each business group. SDMs shall perform the following, at a minimum:

- Incident management
- Problem management
- Change management
- Release management
- Escalation management/Service Request status
- Communication
- Billing management
- Availability and capacity management
- On-call rotation

The on-call rotation in which the SDMs shall participate is critical to facilitate centralized after-hours support to the County for issue resolution as well as making sure each SDM has appropriate amounts of time off and vacation as required. Contractor shall provide five SDMs who shall rotate on-call every five weeks. During business hours (Monday through Friday 6:00 a.m. to 6:00 p.m.), each SDM shall be responsible for their own business group. After hours and on weekends, the on-call SDM shall take primary responsibility for any issue and works it to resolution. If an enterprise issue emerges during business hours, the on-call SDM shall take point for this issue initially—and possibly to completion, depending on the scope of the issue. If an issue arises during this time within the business group for that on-call SDM that requires their focus and attention, another SDM shall be assigned to take over the new issue. All SDMs from each business group shall be required to work any/all enterprise related issues/disasters that require a shift rotation. The on-call SDM shall verify that the correct customer from the business group is notified and that the SDM assigned to that business group is aware if anything has occurred in their space so they can address it. Problem management is a day-to-day responsibility for the SDMs, and they shall be assigned activities to work whether it be proactively or through tickets, escalations, and so forth. Contractor's enterprise problem manager shall report, track, and communicate all problem management issues worked by the team and the account as required in the weekly CTO Operations meeting. Each SDM shall also report any problems being worked by them through this process that impact their business group or the enterprise in the monthly portfolio review meetings that they shall be required to attend.

For capacity management, each SDM shall be responsible for using report-based findings and data to facilitate the health of their servers and applications for that particular framework. The SDMs shall operate proactively to make certain this health is sustained, reliable, and predictable. They shall work closely with the capacity manager on the

account who owns the activities and verifies that Contractor is resolving alerts as well as reviewing trends to implement the right steps to prevent alerts and to make recommendations to County stakeholders.

Contractor shall have a single point of contact on the account responsible for Root Cause Analysis (RCA), making sure that all RCAs meet the required deadlines and service level agreements (SLAs). As issues are worked—for those that require an RCA or for which an RCA has been requested—the SDM for each business group shall make sure that they are completed within the SLA timeframe and they are ready for customer review and approval.

Each business group shall have regularly scheduled meetings that the SDM shall be required to attend and report status as needed for all things operational and that fall within the scope of their duties. Because the SDM acts as a point of escalation, they shall assist the client with answers and resolutions by establishing the proper points of contact and making sure the issue is being worked or obtaining and providing the information required.

If an emergency or disaster occurs in a specific business group, the SDM for that unit shall take primary responsibility as needed to support the customer. They shall handle the requests, communications, and so forth required for these events. If the event is something that requires 24x7 support, Contractor shall provide the necessary resources to cover shifts and see that the SDM has adequate support. If an emergency is declared that impacts the entire County and the Office of Emergency Service (OES) activates, the SDM for the Public Safety Group (PSG) shall begin the rotation along with the enterprise service delivery manager to establish required communication and coordination, and the SDMs shall enter that rotation along with Contractor account management to support the effort until Contractor is notified to stand down.

The ESDM shall be responsible for leadership of all SDMs and shall provide continuity across the business groups and the account. The ESDM shall have a direct interface with the County Technology Office (CTO) to make sure that all parties are aware of anything that is going on in the environment and to make process changes/suggestions as needed for continuity of operations. The ESDM shall be embedded with the customer three days per week in the CTO and shall attend all business group meetings as requested. The ESDM shall be responsible for all delivery aspects and SLAs associated with each area for the account on the operational side: service delivery management, Service Desk, End-User, infrastructure services (data center and local), print center, network services, release management, change management, problem management, incident management, and configuration management.

The SDMs shall be responsible for understanding all service frameworks and how they impact their business group as well as for making certain that proper communication and discussions for that framework take place and that resources are available to support all service delivery initiatives. The SDMs shall be familiar with and facilitate adherence to County requirements and information infrastructure.

- Deployment plan for resources and use of facilities

The SDMs are required to have face-to-face interaction with their business groups in addition to email, phone, etc.

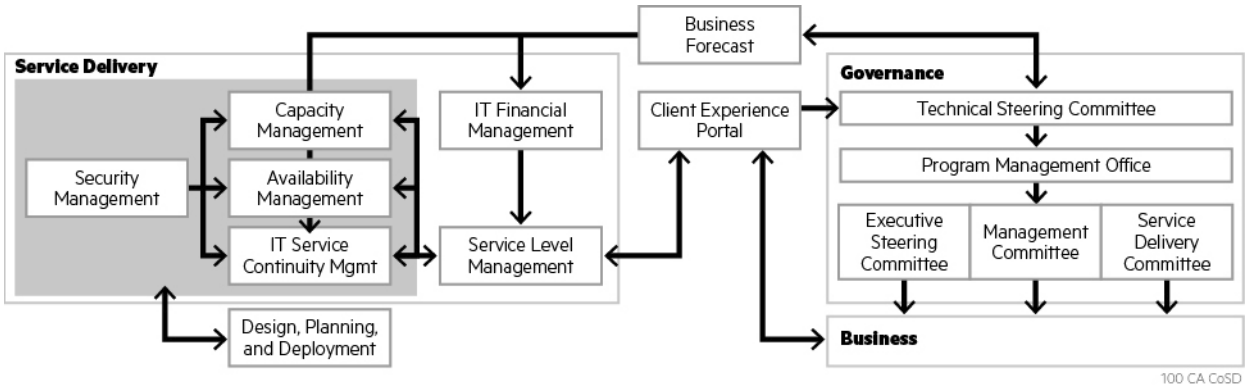
- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's approach to service delivery, illustrated in the figure below, shall enhance the stability and integrity of the services environment through proactive service-level management and governance, transparent service visualization, and analytics that support cost-effective service improvements through integrated availability, capacity, IT service continuity, and financial management. They shall include the following key service delivery disciplines:

- **Availability Management** – The mission of availability management is to understand the availability requirements of the County and to plan, measure, monitor, and continually strive to improve availability of the services and the County's IT infrastructure.

- **Capacity** – Contractor performs capacity planning regularly as well as when new business and application growth are anticipated, when changes to the existing business are anticipated or occur, or when configuration changes are performed within the systems. As part of Contractor's ongoing capacity review and planning process, Contractor shall coordinate with the County regarding future business plans and computer resource requirements.
- **IT Service Continuity Management** – Contractor's business continuity professionals shall collaborate with the County to keep its IT Service Continuity Management (ITSCM) plans current, relevant, and executable and to see that they support County operational continuity plans.
- **Service Level Management (SLM)** – The County and Contractor establish a shared view of the services, service-level achievement, and analytics through regular service delivery reviews and IT Service Management (ITSM) Client Portal dashboards. Contractor's account leadership team shall collaborate with County stakeholders through service delivery reviews and frequent direct dialog to continually review SLAs to make sure that services remain cost-justified and aligned to the County's business needs. The ITSM Client Portal provides continual "Voice of the Client" feedback to Contractor and relays performance feedback at any time, with top-level visibility to Contractor's senior leaders.

Contractor's Service Delivery Model



Service delivery integrates availability, capacity, IT service continuity, IT financial, and SLM to enhance the stability and integrity of the services environment.

The following sections provide additional detail about the service delivery processes depicted in the diagram and summarized in the figure above.

Availability Management

Availability management shall contain the following key activities:

- Assess availability requirements
- Develop and maintain the Availability Plan
- Analyze current availability
- Maintain availability

Capacity Management

Contractor shall perform capacity planning regularly when new business and application growth are anticipated and when changes to the existing business are anticipated or occur, and when configuration changes are implemented in the systems. Capacity management shall meet the following key objectives:

- Verify that optimum IT capacity exists always

- Proactivity
- Reliability
- Outage prevention
- Provide clients with sufficient capacity to support agreed levels of service
- Forecast future requirements for IT resources.

Service Continuity Management

Contractor's business continuity professionals shall work with the client to be sure that ITSCM plans are current, relevant, and executable and that they support the County's business continuity plans. The ITSCM process shall be comprised of the following key elements:

- **Define, Implement, and Maintain the ITSCM Plan –** Contractor collaborates with client business continuity teams to define, implement, and maintain an ITSCM plan that is based on Disaster Recovery Institute International (DRII) and Business Continuity Institute (BCI) standards. The plan is continually updated and assessed through scheduled reviews, as changes are made to the IT environment and as improvement opportunities are identified through testing and execution of the plan.
- **Exercise and Execute the ITSCM Plan –** Contractor's IT service continuity staff shall support the client when conducting required testing and activating plans during a disaster. Contractor shall document and maintain the Contractor staff's IT service continuity procedures to restore the hardware and operating system and the subsystem environment. Contractor operations shall support application recovery testing, such as loading tapes or initializing data storage devices. Joint testing of the IT service continuity plans is conducted through a disaster simulation process based on established test schedules. Contractor closely monitors and document test objectives and actual test activities. Contractor reviews the results of each test and enter any problems encountered in the problem-tracking tool for follow-up and implementation of corrective action. This process enables continual improvement of the recovery plans. Retests shall be performed for tests that do not meet predetermined objectives unless mutual agreement deems retest to be unnecessary.
- **Manage Service Continuity Escalation –** Throughout a service continuity event, Contractor shall manage the agreed escalation procedures to keep the client and Contractor leaders informed, obtain required approvals, and restore service operations in accordance with service levels, thereby minimizing the impact to business operations.
- **Supplemental Assets –** Available for use on the County's program, Contractor has ITSCM-based templates for documenting the following: Business Impact Analysis, Gap Analysis, Continuity Planning Checklist, Threat Analysis, ITSCM Plan, and ITSCM Exercise Workbook.

Service Level Management

Contractor shall work with the client to verify that the levels of service Contractor delivers meet County business objectives.

Security Management

Contractor shall complete a Security Management Plan (SMP) modified from its proven template to identify those security-critical items whose failure could lead to a breach of system security. Contractor shall document a security assurance strategy to minimize or eliminate the potential for system security breaches. Contractor shall review and update the SMP as necessary throughout the program life cycle.

Approach to the role of the Service Delivery Manager (SDM), including SDM operational authorities across Service Frameworks, key functional activities, and metrics to measure the effectiveness of the SDM role.

The SDM shall work closely with counterparts from the County team, outside vendors, and Contractor teams to facilitate a successful initial and ongoing services delivery engagement. This role—essential to managing a small team of technical and business people—shall require varied expertise in the areas of technology, business

processes, communications, service provider, and enterprise IT industry knowledge and experience. SDMs shall serve as the face of Contractor services on an ongoing basis for the County in all aspects from supporting pre-design activities and design to delivery, process improvement, and escalation management."

SDM responsibilities and deliverables shall include the following:

- Serves as primary interface for all client contact related to the Contractor services, involved in pre-design and post implementation interface with County and Contractor services leadership teams
- Responsible for County relationship management and total customer experience
- Works closely with senior management and across functional groups to develop effective strategies and programs to meet service delivery goals, including tracking and reporting key milestones
- Responsible for making certain that Contractor complies with agreed services scope and quality
- Provides compliance with established policies, practices, and processes defined by Contractor and County personnel for delivering converged infrastructure related services
- Provides work direction and strategic direction to reporting managers and employees
- Works closely with Contractor lead partners in ensuring a successful services delivery engagement

Metrics to measure SDM effectiveness shall include the following:

- County leadership evaluations—the GITM and ESDM shall meet quarterly at a minimum to discuss how the SDM is providing the services required
- Project performance to goals and objectives
- Meeting scheduled reporting and communication deadlines
- Maintaining agreed certifications
- Annual Performance Reviews by the ESDM
- Customer relationship management skills and meeting objectives
- Identifying opportunities for improvement within their respective business group

2.8. [Reserved]

2.9. Project Management Services

2.9.1. Process and Procedures

- Description of solution to meet the requirements

The Contractor Enterprise Project Management Office (EPMO) is an organizational body that shall be assigned to centrally coordinate the management of in-flight programs and projects across all towers of the Agreement.

Solution: The EPMO shall be responsible for aligning its activities with the County's mission and maintaining an outcome-focused and metric-centric program management organization. To accomplish this, Contractor shall incorporate measured steps to retain situational awareness of the budget, schedule, and risks as well as opportunities for continual improvement throughout the program's life cycle. The EPMO strengthens day-to-day communications and prepares detailed recurring reporting to promote the highest level of transparency and collaboration between the County and Contractor.

Contractor shall use industry-standard practices as set forth by the Project Management Institute (PMI's PMBOK), Software Engineering Institute (SEI's CMMI), and Information Technology Infrastructure Library (ITIL). Contractor has its own Enabling Delivery and Global Excellence (EDGE) process, which is its overall framework for enhancing effective planning, execution, tracking, and reporting of projects. The Contractor team shall use one or more of these best practice standards to create procedures that enable each framework to efficiently perform project management activities appropriate for the nature of its work.

Contractor EPMO guiding policies shall include:

- Identify and use global best practices as a framework for creating tailored, relatable, and customer-centric procedures that provide the best fit to meet Contractor's customers' evolving needs, while driving quality and expedience into Contractor's delivery model.
- Provide frequent, accurate updates to the County Project Sponsor
- Make sure of thorough and timely communication across all framework projects and procedures
- Apply the principle of delivering projects on time and within budget that fulfill the approved requirements
- Promote an environment of continuing education for Project Management Professional (PMP)-certified PMs and for those who aspire to be PMP certified
- Work with Contractor's County partner on continuous improvement processes and initiatives.

These policies are designed to influence and determine decisions and actions when tailoring the processes for the County and ensuring that Contractor's processes conform to PMBOK, CMMI, and ITIL.

The Contractor EPMO person shall chair weekly meetings to make certain that cross-framework coordination, integration, and communication occur for projects and processes. Communication between all frameworks is critical to successful delivery of products and services.

The EPMO shall be committed to coordinating multi-framework projects between the frameworks, and to certifying that there is a lead project manager and project status is reported in a timely and consistent manner. EPMO shall provide a central point for managing processes and standards across all frameworks to enable consistent delivery.

Contractor shall use a formal process change board to identify and implement process improvements that drive quality and expedience throughout the project life cycle. The HPE EPMO shall chair these efforts and support documentation, training, and process reengineering that may be identified through these efforts.

In addition to the standard project management solution described above, Contractor shall consolidate Infrastructure Project Management efforts into its project management service. This provides value to the customer while continuing to facilitate Contractor's goal to integrate all project management services under one set of best practices.

Rationale:

The EPMO shall drive the standards for project management across all portfolios, but shall remain agile where necessary to meet the needs of the specific project/client.

- Deployment plan for resources and use of facilities

The EPMO and project management staff shall be centrally located at the Contractor's Rancho Bernardo facility. Contractor shall join the County at its facilities when necessary to drive successful communication at the program and project levels. This facility approach enables interaction between the project management staff and all customer and Contractor portfolio towers, including:

- County Technology Office (CTO)
- County Group IT Management (GITM)

- County Department IT Coordinators
- County Project Sponsors
- Contractor Account and Operation Management
- Contractor Applications Portfolio Management
- Contractor Infrastructure Operations
- Contractor Account Security
- Contractor Technology Office
- Contractor Business Management
- Contractor Contracts Management

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's proven methodology for effective program management support, EDGE, includes all information needed for Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE shall support all individuals in each ES business unit by providing best practices that they can leverage and use in their daily work.

The EDGE environment shall cover multiple life cycles that can be selected, customized, and integrated as needed for each program. Project and program management shall be integrated through their own life cycles, which conform to PMI PMBOK industry standards, as well as CMMI and ISO. Engineering practices, such as Infrastructure, COTS, and other Enterprise application areas, shall integrate seamlessly with the Project/Program Management areas for project success. EDGE has been customized to the County's needs and processes. EDGE shall be regularly updated to provide End-Users with the most current industry best practices, as well as continually aligning processes and assets with changes in industry standards of PMI, CMMI, ITIL and ISO.

Using the aligned HP/County organizational structure, Contractor shall implement formal communication procedures that engage internal and County stakeholders. Examples of interactions include the following:

- Establishing communication strategies for the specific needs of the CTO and County business groups
- Developing enterprise communication procedures and templates
- Auditing program and project communication plans
- Creating EPMO announcements followed up by direct communication with impacted stakeholders
- Developing and maintaining communication vehicles such as the EPMO SharePoint
- Creating and executing communication plans for EPMO initiatives
- Preparing presentation material for internal and external reporting.

Standardization and optimization of Project Management practices across a diverse environment such as the County

The Contractor EPMO and County CTO partner shall be responsible for the integration of these processes across the County enterprise so that service performance can be managed seamlessly. Contractor's EPMO personnel shall facilitate the development of processes, manage the deployment, and provide oversight and management for process execution. Contractor's EPMO personnel shall also establish key roles for ownership and governance of each process, working collaboratively with the County to speed delivery of services focused on quality and adherence to standards.

Internally, the project management team shall meet regularly to escalate issues and to discuss project management measurements and trends. They shall receive training on updates to client processes, industry best practices, and new tools. Contractor additionally shall monitor and meet with subcontractors to make sure they comply with County and project requirements. Contractor shall make certain that subcontractors are aware of and participate in issue and risk management, and that they provide timely accurate status reports.

Contractor shall provide training for project managers, including acceleration programs for the PMP, CAPM, SPI, and other disciplines. Project managers and business analysts shall be encouraged to join and participate in global, regional, and Community of Practice (CoP) groups, including the USPS PPM Community, the State/Local

Government / Education (SLED) Community of Practice, and the USPS Business Analyst Community of Practice, for additional training and shared understanding of best practices across the community.

PMI chapter and PMI/PPM event participation shall also be encouraged across the organization.

Contractor's PPM Academy shall provide regular opportunities for learning.

The EPMO shall share in-house opportunities for PM training sessions or vendor sessions, or PM-specific conferences in San Diego, and inform the County that it may participate.

Contractor shall leverage the best practices of Project Management Plan development and right-size the project for specific County needs. Project Management Plans shall contain one or more of the following sections:

- Scope Statement
- Known Risks and Issues
- Assumptions and Dependencies
- Stakeholder Matrix
- Milestones
- Cost/budget Baselines used in calculating SLs and project success
- All Project Deliverables
- Preliminary Risk Log
- Phased Implementation Approach.

Project schedule templates shall be maintained in the Program and Project Management Center (PPMC). Each framework shall have one or more templates that meet the needs of their particular project tasks.

Contractor shall conduct risk analysis and planning early in the project life cycle with the help of all stakeholders. Monitoring risk and updating the risk matrix shall occur continually during the project life cycle.

For the Applications and Infrastructure frameworks, change management shall follow the formal change request process that flows through CTO and is signed by County and Contractor.

County-facing project status reports shall be made available so that authorized County users and Contractor team members can view the status of a particular work request. Status reports for projects shall be posted on a weekly basis.

All PM work products, status reports, processes, and templates shall be centrally located/managed and shared using DocVault.

Each project manager shall be responsible for establishing and conducting project meetings with his/her customer.

Third-party vendors working with Contractor to implement solutions shall be treated as project team members and held to the same process standards required by the County and Contractor. From the point of project kickoff, the Contractor project manager shall be responsible to direct County vendors on their roles and responsibilities for supporting County projects and required deliverables. These responsibilities shall include following County-approved methodologies and processes and any project status reporting requirements.

In addition to requiring all vendor project participants to follow County-approved project process, Contractor shall also identify potential project risks as part of the upfront project risk assessment and shall include specific mitigation plans for issues that may arise when operating a project that uses third-party vendors. Those risks shall be managed and monitored for risk triggers throughout the project lifecycle.

Measuring and analyzing trend data related to the effectiveness and timeliness of Project Management processes and methodologies.

The Project Management Office shall work directly with County representatives to recommend and identify the critical performance indices that provide useful project trends and status. Project trends shall be calculated and reported on a regular basis by the Project Management Office and discussed as part of weekly project review meetings. Trends related to project schedule, budget, and other key performance indicators shall be monitored on active projects in Contractor's Project and Program Management system. If Contractor identifies unfavorable trends, it shall perform a root-cause analysis to isolate new causes of trends, and provide coaching assistance to project managers to understand the root-cause and provide corrective and preventive action.

The County has designated two critical SLAs around the KPIs of Schedule Performance Index (SPI) and Cost Performance Index (CPI) on Discretionary Standard projects. Contractor shall support these KPIs throughout the project lifecycle, measuring progress and reporting on earned value. Contractor shall constantly manage to these metrics throughout the project lifecycle.

Contractor shall implement the following or as otherwise stated in the Standards and Procedures Manual:

- KPIs for Project Estimate Accuracy and Response
- KPIs for Impact, Priority, and Mitigation of Risks/Issues
- KPIs for Project Change Management
- KPIs for Projects Opened, Closed, Delivery Times, etc.
- KPIs for Defect Management
- KPIs for Project Schedule Management/Milestone Comparisons

Contractor shall continue to identify additional KPIs best suited for the project management organization. The County and the Contractor PMO shall meet regularly to discuss overall objectives, issues, and improvement items, which can be incorporated into ongoing KPI development and improvements.

The Project Management Office shall use tools to collect and measure the effectiveness of estimates against actuals for all standard projects from initiation to closure. Contractor shall review trend reports regularly, along with individual reporting per project. The data collected shall include estimates at initiation, actuals by role at closure, total project CPI/SPI, number and type of change requests, and cost impacts. Contractor shall also collect data to determine the effectiveness of ROM estimates for project management and engineering project activities and continuously update the Basis of Estimate process and provide more accurate and predictable ROM estimates.

Relationship between project managers and Service Framework resources

Where possible, the same project resources engaged for creating project ROM estimates shall also be responsible for delivering the end product. This approach drives a high level of accountability and quality for Contractor's solutions.

Starting with the project's initial estimate, Contractor shall engage the solution frameworks to provide rough estimates for the project's proposal. Once a project is approved by the County, Contractor shall initiate an internal kickoff with the team, and the project manager shall engage the framework leads to determine the level of resources and effort needed from the initial requirements gathering through deployment. Requirements Development and Planning shall engage the framework resources to refine the solution and further refine the estimate of resources needed to deliver. During execution, testing, and deployment, the various frameworks shall be actively engaged in providing and testing the solution, and positioning for, executing, and supporting deployment. At project closure, the framework resources shall continue their involvement to make certain that warranty-period support is available, turnover to production is successful, and project close-down ends with a

final collection of effort and lessons learned. These touchpoints shall be embedded in the standard project plan templates and reflected in the project management life cycle.

Throughout this processes, Contractor shall identify framework SMEs from operational support when needed to advise and provide critical product information and input to the project team while supporting the operational needs of the product.

Use of Tools

Project and Portfolio Management Center (PPMC) shall be Contractor's Primary Project and Portfolio Management (PPM) tool suite. Contractor shall use PPMC for the development and ongoing management of project schedules, small project work, LOE-based work, operational support work, budget tracking, and status reporting. Contractor shall also use it to track program-level, high-visibility initiatives with multiple projects, and at the portfolio level to manage and track projects with competing resource needs within a business group.

- Contractor shall use SharePoint as a storage repository for project artifacts, enabling easy access of project standards, methodologies, processes, and procedures; storage and access of project templates; and storage and access of project-specific documentation such as specifications, project plans, etc.
- Basis of Estimate: Contractor has developed a unique Rough Order of Magnitude (ROM) tool that the EPMO shall use to support expedited and thorough estimates that the County needs to secure funding for its initiatives. This tool is based on PMBOK-defined procedures for estimating while accounting for County-specific processes when developing an estimate. It enables the project manager to define the project work in terms of complexity/risk and a standard list of deliverables and tasks which follow the development methodology selected and client requirements at the early stages of a project. It provides ranges of estimates based on the input and historical estimates and actual effort from past projects. This customized tool takes into account client and Contractor processes and life cycles, and documents decisions and assumptions made for planning. This tool is managed internally, and automates the creation of client-facing deliverables, including the Budgetary Estimate Cover (an authorizing document). The EPMO team tracks performance of estimates to actuals on projects and uses that data to further inform and improve the BOE tool and improve the quality of Contractor's estimates to the County client.

The following table shows additional Contractor automated tools and methodologies.

Contractor Automated Tools and Methodologies

MANAGEMENT TOOLS AND METHODOLOGIES	FUNCTION	
Service Portal	Acts as the single, virtual, and centralized source of information for all County stakeholders and HP. The Portal shall provide access to the following:	
	• Consolidated program reporting • Service levels reporting	Contractual information Contractual deliverables and plans
Project and Portfolio Management Center (PPMC)	• Consolidated project management tool • Budget management and labor billing source • Schedule management • Resource management • Risks and issues management • Project status reporting	

MANAGEMENT TOOLS AND METHODOLOGIES	FUNCTION
County Document Repository (DocVault)	Workspace and final repository for all project-related deliverables and account-wide policies and procedures
Program and Project Management Methodology	Includes templates that outline scope, risk, quality process, personnel, cost, schedule, communication, and procurement management responsibilities
Service Delivery Dashboard and Voice of the Client (VoC)	Provides clients with program performance and enables them to provide direct feedback to Contractor executive leadership

For internal tools such as the above that are used to the support the County's business, Contractor shall conduct reviews of the systems on a semi-annual/annual basis, depending on the tool, to determine whether major upgrades or replacements of systems are required to make certain that Contractor is using the right technology to support the County's needs and remain in supported status.

2.10. Integration and Testing Services

2.10.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall use a comprehensive testing framework that includes the structure, processes, tools, and templates to enable consistent, high-quality testing services and deliverables. Contractor's testing framework shall verify compliance with the application development process and shall validate the quality of the application to address the commitments outlined in the SOW. Contractor shall achieve maximum integration testing efficiency by grouping testers separately from developers.

Contractor shall first work with the County to determine the level of strategy that best meets its needs. Contractor shall review the current strategies, testing requirements, business needs, and priorities to develop the most efficient and cost-effective testing strategy for the SOW project.

Contractor shall supplement and support the project life cycle with the following testing-specific information:

- Testing roles and responsibilities
- Testing methodology
- Test levels to be performed
- Test coverage to be performed for each test level
- Test deliverables
- Test management and measurement approach
- Required testing environments and tools.

Based on the priorities identified in the test strategy, Contractor shall develop a Test Plan that covers each required test level and provides tactical guidance by specifying the following factors:

- **Test Scope** – Scope of Contractor's testing services to be provided, including test types
- **Test Schedule** – Schedule for all phases of testing, integrated with the overall project schedule (test development, test execution, testing metrics collection, and testing reporting)
- **Test Roles and Responsibilities** – Test roles/responsibilities for all participants, including the Contractor team, County staff, and third-party vendor staff; responsibility for test environments and tools
- **Test Design/Methodology** – Test case design techniques/strategy for each test level

- **Test Procedure/Execution** – Test-level execution tasks, including participants, to conduct execution; entry, exit, pass/fail, suspension, and resumption criteria for each test level
- **Test Tracking and Reporting** – Test results data collection requirements, documentation, and reporting; test progression tracking and error/deficiency management/resolution process; risks specific to a test level that require mitigation.

The Contractor Test Plan shall also outline the recommended testing tools and testing management and measurement.

Contractor shall apply and adapt the processes, techniques, and templates of its testing method to effectively manage and control the planning, execution, and completion of all testing activities. Testing management and measurement shall involve the following actions:

- Establishing and maintaining detailed estimates, a test schedule, resource plans, and procedures for all testing phases
- Managing preparation of test plans, scenarios, and test cases for each test level
- Establishing acceptance criteria
- Managing the execution of test cases, tracking and resolving defects, and verifying completion of tests, including regression testing
- Managing testing close-down, including reporting.

To make sure the application is ready to move into production, Contractor shall apply comprehensive metrics, supported by standard testing management tools. Contractor shall generate reports to provide insight into the status of testing throughout the project. With this information, Contractor shall confirm that tests are mitigating risks on high-priority requirements. These metrics shall support timely corrective action and informed decision-making by all project stakeholders, particularly "go/no-go" decisions to progress through project phases.

System testing shall involve testing both an application and its supporting infrastructure. Contractor shall provide system testing to establish confidence in End-User acceptance of the system and that the system is functionally and structurally stable, reliable, secure, and interoperable. System testing shall encompass an integrated system or a logical subset of application functions. It shall verify compliance with functional and nonfunctional system requirements and specifications. The process normally involves creating test conditions for evaluating the application and its infrastructure.

Contractor shall prepare and perform system tests based on approved requirements documents, the application architecture, and the application design specified by the development team. Contractor shall create tests to exercise the specific business functions selected and submit them for County approval. This approach helps to validate that the system performs according to the County's requirements.

System testing shall include testing interfaces with external entities and with batch and online software. All parts of the system shall be available for system testing to succeed. Data shall enter through normal interfaces so Contractor can test interaction between various subsystems. If the County does not have an appropriate testing environment available to accept transactions or files, Contractor may use emulators to simulate interactions with external systems. System test activities shall include the following:

- Test cases, standard and ad hoc
- Test data management
- Requirements Traceability Matrix (RTM)
- Performance benchmarks when applicable
- Summary report.

Contractor shall use automated life cycle management (ALM) tools and techniques as it develops system test cases based on functions and roles. Function-based tests validate the application's functional requirements and

data flows. Role-based tests shall verify access to the application, menus, submenus, buttons, and icons; verify a complete and correct process flow for each defined role; and validate that access covers only specified areas.

The following table describes Contractor's high-level input criteria, activities, and deliverables for test cases.

Contractor Test Criteria and Deliverables

INPUT CRITERIA	• Baselined test scope, strategy, and plan • Baselined effort estimation and schedule • Baselined defect, change, configuration, communication plan, and risk management plan • Baselined and updated Test Traceability Matrix (TTM) Baselined design, business requirements/specifications, and use cases documents
ACTIVITIES	• Identify functional and technical test scenarios • Update affected test case and script • Design new test cases and scripts: review, sign off, and baseline • Define success criteria and expected outcomes • Design test data: review, sign off, and baseline • Collect metrics Update test traceability, arrive at test coverage, and sign off
DELIVERABLES	• Baselined test cases, scripts, and test data • Baselined smoke test suite • Baselined test traceability Sign-off by stakeholder

Contractor shall implement the database approach to test data management.

The RTM shall trace downstream work products of the requirements, such as design, code, and test cases. If an RTM exists, the Contractor testing team shall update it when the initial test design is complete, to map requirements to test cases. If an RTM was not developed, Contractor shall establish one while developing test cases, linking each test case back to the original requirement.

As Contractor executes test cases, it shall document and map any defects it encounters to the corresponding requirements in the matrix. The updated matrix shall provide a running record of how testing has addressed and met each requirement, revealing gaps the testing team needs to fill and opportunities to consolidate redundant tests.

The County shall receive a complete overview of system testing results in a system test summary report, which shall include an overview of the approach, tools, test cases, activities, results, and any outstanding defects.

System integration testing shall confirm that the necessary communications and setup exist to perform functional testing and shall address the need to assess whether the system interfaces smoothly with other applications or systems.

After the development team provides the testing team with the interface code, Contractor shall perform system integration testing. This testing is often the most complex because it normally involves communication and security layers and requires coordination with outside organizations.

Certain applications may involve providers external to the individual SOW. When testing with an external organization, Contractor shall provide that group a copy of all test cases to review to support test coordination and data synchronization. To support external interface testing, Contractor shall work closely with the County project manager to coordinate and cooperate with third-party interface owners.

In conducting performance testing, Contractor shall 1) understand the performance requirements; 2) determine the types of performance tests and the test volumes that best meet those requirements; 3) test the system performance; and 4) ensure the new change does not impact existing functions or systems. Contractor shall also assist the County with performance tuning recommendations to help fix performance-related issues. Contractor's methodology shall include the following actions:

- Identify and scope requirements
  - Performance test requirement analysis, review of volume metrics and performance goals
  - Performance test strategy and planning
  - Arrive at scope effort, cost, and timeline
- Determine performance testing type
  - Load testing
  - Stress testing
  - Volume testing
  - Scalability
  - Failover testing
  - Regression testing
- Review and provide recommendations of performance test scenarios and volume metrics performance goals provided by the project team
- Develop performance test strategy, test plan, and scripting standards
- Set up and maintain the test environment, including build and deployment activities
- Prepare test data for project owner's review before baseline
- Design, execute, and analyze performance test for approximately four performance test scenarios identified and provided by the project team
- Provide required support for the performance tuning team, such as re-execution of scripts to identify replicating issues.

The following table presents detailed performance and load-test strategy.

Contractor Performance Testing

PHASE	INPUT/ENTRY CRITERIA	ACTIVITIES	DELIVERABLES
Discovery Phase (Requirements Analysis and Performance Test Planning)	• Application non-functional requirement specifications (SRS, design specifications, and so forth) • Business scenarios, performance test scenarios, use cases • Performance goals and volume metrics • Release scope • Production environment details	• Conduct requirements study • Determine test scenarios and impact analysis • Identify test scenarios for performance testing • Develop performance test strategy/plan • Derive test environment specifications • Conduct performance test scenarios, test strategy/ plan, traceability, review, and approval	• Performance test strategy/plan • Identified test scenarios for performance testing

PHASE	INPUT/ENTRY CRITERIA	ACTIVITIES	DELIVERABLES
Performance Test Environment Preparation/ Readiness	• Performance test strategy, plan • Tools and licenses • Application builds • Performance test environment • Functional test cases • Performance test scenarios, test cases and test data, sample test data • SRS, design, other specifications	• Set up and configure test environment • Deploy and configure application build • Identify performance testing tools, monitors, installation, and setup/configuration • Test data preparation, review, and baseline • Test environment and build validation through sanity testing	• Performance test environment with latest build • Performance test data • Performance test tools installed and configured
Performance Test Design/ Development	• Performance test scenarios • Identified performance business scenarios • Performance test plan • Test environment with latest stable build • Performance test data • Performance test tools installed and configured • Baselined performance business and test scenarios	• Develop performance test scripting standard • Develop performance test framework • Develop test scripts/test suite (integration of test scripts) • Develop test data files • Identify and review performance test metrics • Review and baseline all above test artifacts	• Performance test framework/ harness • Baseline performance test scripts and test suite(s) and associated test data and configuration files
Performance Test Execution, Analysis, and Reporting	• Performance test strategy and test plan • Test environment with latest stable build deployed • Baseline test scripts • Non-functional requirements (performance goals and volume metrics) • Test environment sanity test and all test entry criteria	• Validate test entry criteria • Execute performance test • Validate test exit criteria • Analyze and report performance test results • Collect performance test metrics • Log and track defects	• Performance test execution status reports • Performance test results, performance issues, bottlenecks, metrics reports • Sign-off report
Performance Tuning Support and Post-Tuning Testing	• Performance test results and reports • Performance test results analysis report and recommendations for tuning • Performance goals and volume metrics • Test entry/exit criteria	• Validate test entry/exit criteria • Provide performance-tuning support • Provide post-tuning retesting of scripts • Conduct result analysis of post-tuning tests • Provide performance test reporting for post-tuning tests	• Post-tuning test results • Post-tuning performance test reports • Final sign-off on performance test report

To identify and correct vulnerabilities before the application goes into production, Contractor shall provide Security Testing Services, which shall make sure the County's applications are protected against exposure to hackers or other threats to their integrity, availability, or confidentiality. Security Testing Services shall help the County achieve the following goals:

- Improve coding and security practices
- Identify and eliminate or mitigate security vulnerabilities in web applications
- Comply with regulatory and reporting requirements
- Test existing applications and quickly address major vulnerabilities
- Cut overall project costs by identifying problems early.

To address security risk levels associated with unique applications, Contractor shall provide vulnerability code scanning and application security testing. Contractor shall work with the County to assess the application risk level, then recommend the types of security testing required.

Contractor shall provide vulnerability code scanning for medium-security-risk applications. First, Contractor shall scan the code to identify critical vulnerabilities, then Contractor shall assist the development team with remediating issues and applying regression testing code fixes to address these vulnerabilities.

Contractor shall provide application security testing in the testing environment for high-risk web applications to uncover security vulnerabilities before moving the application into the production environment. Contractor shall assist the development team with remediation and regression testing of code fixes to address the vulnerabilities uncovered.

Regression testing shall involve selectively retesting previously tested functions and running selected test cases to make sure that new development and defect fixes have not introduced or revealed new faults. Regression testing can occur throughout testing and shall be executed whenever the build changes. It shall occur at all test levels of Contractor's Enterprise Testing Methodology and throughout development.

During test case development, Contractor shall identify candidates for regression testing. Contractor shall then use these cases to test future application releases. The following changes shall typically require regression testing:

- Addition of new business functionality (new modules or sub modules, new business transactions, new business processes)
- Modifications to current functionality (enhancements, defect fixes) for a release
- Implementation of the current application to new locations
- Upgrades to more recent versions of the application or operating system
- Hardware upgrades.

Business regression testing shall focus on the critical, high-volume business processes for all business functions introduced, up to or including the previous software release. Contractor shall build on previous regression tests by adding new scripts with tests based on the last release's functions. Contractor shall focus specifically on known high-risk areas.

Contractor shall provide the option to perform regression testing after completing a major type of testing (such as system testing) but before releasing the application to the next test level.

- Deployment plan for resources and use of facilities

Contractor's key facilities shall be in Rancho Bernardo, CA; El Paso, TX; Pontiac, MI, depending on skillset required.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's testing methodology shall align with the industry-accepted Testing V-Model.

Contractor's risk-based, requirements-driven testing approach includes the following components:

- **Ambiguity Analysis** – While performing requirements validation, Contractor shall systematically analyze ambiguities in the requirements that drive application design, development, and testing to minimize

inconsistencies and maximize clarity. This process helps to meet users' expectations; gives the project team a targeted and complete plan; and builds common understanding of requirements for project managers, developers, testers, and users.

- **Risk Analysis** – Risk-based testing shall focus on analyzing risks to reduce misdirected or incomplete test coverage. Contractor shall systematically analyze requirements to determine the priorities that guide the testing strategy. All stakeholders, including third-party interface owners, are engaged in these analyses. Contractor shall define test environment requirements early in the life cycle.
- **Systematic Test Design** – Through methodical activities focused on managing and mitigating risks, Contractor shall apply test design techniques to plan, choose, and develop the most effective tests to deliver the required amount of testing.
- **Requirements Traceability** – Throughout test development and execution, Contractor shall update the RTM to comprehensively depict test coverage and to keep testing focused on high-risk, high-priority requirements. Because each test case inherits priority from its requirement, the RTM helps the team analyze the testing impact of any requirements changes.
- **Testing Metrics Collection/Reporting** – Contractor shall use testing reports to gain ongoing insight into the progress of tests and defect resolution, and Contractor shall offer timely opportunities for mitigation of a risk before it causes harm to the County's environment – or to the application itself.
- **Testing Close-Down Activities** –Contractor shall focus on satisfying high-risk, high-priority functionality first through risk-based testing, leaving as the last priority tests and defects for only low-risk, low-priority requirements as agreed to by the County. As part of project close-down, Contractor shall either transition the work to the County, as outlined in the SOW, or continue providing maintenance and support.

2.11. Incident Management Services

2.11.1. Process and Procedures

- Description of solution to meet the requirements

As a part of this process, all incidents shall receive prioritized attention, depending on severity, Service Level Agreement (SLA), or the immediate service restoration needs of the County.

Solution: Contractor shall use an IM process that includes ITIL methodology.

Contractor's focus shall be:

- Restoration of service operations as quickly as possible using repeatable streamlined processes and escalation points
- Frequent, clear, and concise communications to End-Users and CTO through resolution
- Minimizing the adverse impact of incidents on the business
- Providing departments and End-Users with a single point of contact (POC) for all incidents reported
- Maintaining portal-based visibility into incidents and trouble tickets with drill down to detailed information.

Contractor shall provide full life cycle IM through its Service Desk and IM functions. The Contractor Service Desk shall act as the initial POC for the identification, categorization, and tracking of all County incidents in its service management system. This system shall provide the efficient assignment of incidents for resolution by the responsible teams and direct access to incident status by County personnel. The system shall also objectively measure accountability for all aspects of the IM process.

- Deployment plan for resources and use of facilities

Incident management shall be supported by the following groups:

- Service Desk
- Service Delivery Managers
- Applications SMEs
- Datacenter SMEs (network, storage, exchange, BUR)
- Local account server team/Infrastructure SMEs
- Desktop and Remote Support Technicians, as needed
- AT&T
- Engineering and Architecture

The majority of the services provided by this process shall be supported by the account team at Contractor's Rancho Bernardo site; AT&T shall provide services from Trade Street site.

Supplemental support for datacenter and other areas supported by leveraged frameworks shall be provided by the account team in Rancho Bernardo. The Service Desk shall provide support from Pontiac, MI.

- Key methodologies and processes in solution including year-to-year continuous improvement

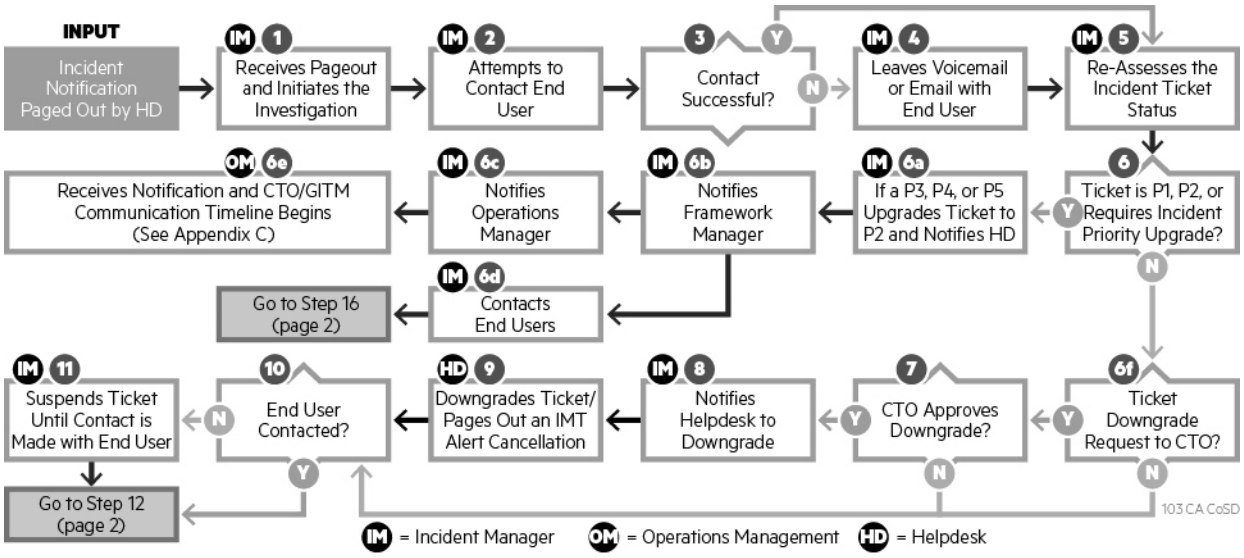
The Service Desk shall serve as the primary point of contact and owner for the identification, categorization, monitoring, and tracking of all County incidents within Contractor's service management system, providing efficient assignment of incidents for resolution by responsible resolver teams and direct access to incident status by County personnel. The system shall also objectively measure accountability for all aspects of the IM process.

The Contractor SDM team shall continually monitor incidents, responses, escalations, and resolution activities through the ticketing system for compliance with procedures and performance objectives. The Contractor SDM shall provide key configuration items (CI) for incident components. During major (high severity/scope) incidents, the SDM team shall actively facilitate status notifications and escalations to all appropriate levels in customer and vendor organizations. Contractor shall provide the right people, processes, and tools to perform comprehensive IM for the County, who shall receive timely responses to questions and issues as they occur and progress through the incident life cycle.

The Service Desk and SDM team shall refine a mature process for full life cycle IM. Each sub-process and step is described in the figure below. This process shall assign Level 1 support responsibility to the Contractor Service Desk, which shall also be responsible for incident recording, categorization, and assignment. The Enterprise SDM shall act as an escalation point and operations orchestrator, helping the County achieve continued high levels of service and End-User satisfaction.

The Contractor enterprise SDM shall be responsible for verifying prioritization and categorization standards for IM processes in collaboration with the County, validating that Contractor records these standards in the policies and procedures and continuously monitor other service providers' compliance with these standards. The Contractor team shall also be responsible for verifying procedures and mechanisms for handling, expediting, and communications of high-priority incidents. These procedures and mechanisms shall be recorded in the Standards and Procedures Manual and also be continually monitored for compliance.

Incident Management Flowchart



The Contractor SDMs shall continually monitor and review incidents within the ticketing system for completeness, accuracy, proper categorization, and timeliness of resolution activities as established by the County and Contractor and defined within the policies and procedures within their respective business groups. Each SDM shall provide operational data and information related to outages and issues, among others, for their respective Business Group. The SDM shall, on a weekly basis, provide reporting of this review to the County Technology Office, operational POCs during the existing weekly Operations status meeting.

Contractor shall continue to document and provide procedures for enhancements related to incident resolution. Scripts, techniques, and step-by-step actions shall be recorded in the knowledge management system, subject to change management processes, for future use by support personnel and End-User access for self-help.

Contractor's IM process shall assign initial responsibility for the identification of problems to the resolving service providers in the problem management process description. If an incident is the result of a change, Contractor shall record the information and refer it to the change management process. If Contractor determines an incident qualifies as a problem, Contractor shall record it in the incident record for referral to the problem management process. Contractor's SDMs shall be responsible for IM and problem management for the business group, and shall verify evaluations performed in this step and escalate incidents to the change and/or problem management process as required.

SDMs shall be responsible for monitoring and managing the entire life cycle of incidents to comply with resolution, status, and notification processes as well as procedure requirements of the Service Desk. As part of Contractor's performance-based management approach to quality assurance, Contractor shall actively monitor and remediate underperforming KPIs and incorporate them into Contractor's continuous improvement process. Contractor shall prepare a quarterly action plan to address service improvement objectives and activities for County review and implementation approval.

Staff and respond to Priority 1 Incidents.

As documented in the County Standards and Procedures, when a Priority 1 incident is received, Contractor shall log it into Service Manager and an electronic alert shall be sent out along with an eNote page to the appropriate

support staff. The SDM on point shall receive the page with the incident ticket number and immediately ensure the frameworks are engaged and have begun work on the issue and preps for customer notification. If services cannot be restored within 30 minutes, a bridge line shall be stood up with all frameworks on the call until resolution of the issue. The SDM shall send the first status to the County End-User and CTO within 60 minutes and the status shall continue every hour until service is restored.

The SDM shall monitor and track the incident ticket to closure and provide all required status communications during the incident life cycle. When a change in the status of the request occurs, the SDM shall determine if the ticket issues have been resolved or if the status change is valid. If issues have not been resolved, the SDM shall continue to monitor and track the request until resolution.

If the ticket issues have been resolved, the SDM shall send out final communication and status and proceeds with next steps based on ticket priority. If the ticket is Priority 1 or 2, the SDM shall make sure that an RCA has been created. When the problem ticket has been completed for Priority 1 or 2 issues or a permanent solution has been implemented for non-Priority 1 or 2 issues, the SDM shall document all the actions taken in the activity fields of the ticket and changes the ticket status to Resolved.

Trend analysis of Incidents to identify and correct recurring Incidents.

The Contractor enterprise problem manager shall be responsible for analyzing quality and reporting trends related to incidents. This analysis shall provide recommendations of appropriate actions to mitigate any negative findings and to propose improvements to drive improved effectiveness and efficiency. As part of the analysis, once a trend is identified, action shall be taken to correct, improve the outcome, or prevent future outages from occurring. These reports shall be provided on a periodic basis. Contractor's proactive method shall include performance-based management and periodic assessments of Contractor KPIs within the IM framework and shall include capturing underperforming mission-critical KPI and SLA metrics, escalating them as necessary, and displaying them on the EPMO status dashboard. Contractor shall also use this data to identify and substantiate trends relating to similar incidents or contributing to problem recurrence, and developing solutions to address chronic issues. Contractor shall continually assess these indicators to identify negative trends. Contractor shall continue to conduct RCAs where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends; thereby ensuring year-to-year continuous improvement.

RCAs

Contractor shall implement the following:

- Once Priority 1 and Priority 2 incidents are resolved, the RCA manager shall enter information into an RCA Submittal Form and submit it to the appropriate SME and framework manager.
- Once received, the Contractor technical SME shall:
  - Gather additional data from other framework SMEs as needed
  - Determine the chronology of events and causes
  - Determine any underlying root and contributing causes and how they manifest
  - Complete the RCA and develop corrective action items/recommendations
  - Complete the RCA Submittal Form and submit findings for Peer and Tower Management Review
  - , submits the findings to the RCA manager once the SME findings have passed Peer and Tower Management Review
- After receiving the findings, the RCA manager shall schedule a formal review by the Contractor RCA team.
- The Contractor team shall then determine if the RCA is complete and, if so, shall address all concerns. The RCA manager shall conduct a final Quality Review and submit it to the RCA team for their final review. On final approval, the RCA shall be submitted to the CTO RCA representative for final disposition.
- This process shall be completed within 6 business days of the final resolution of an incident ticket or receipt of an ad hoc RCA request from the CTO.

- For RCAs related to an outage that is business group specific, the SDM shall make sure all required information is gathered and provided.

Corrective action items that are not completed as a part of the incident resolution in the RCA shall be documented in the Problem Management SharePoint site with an owner and date of completion assigned. This system shall have automatic email alerting assigned to it for the POC to make sure items are completed as required. The Enterprise Problem Manager shall be responsible for validating and verifying that all items are completed on the site within the timeframe that is documented. The HPSM (HPE Service Manager) system shall provide a problem case number for all corrective action items and problems being worked that do or do not have a RCA as a requirement. These Problem cases shall make sure that Contractor has complete tracking and a connection between the incident and the change records required to act on the items that need to be addressed. These cases shall not be closed until all activities are completed and documented.

Detailed processes shall be documented in the Standards and Procedures Manual.

2.12. Problem Management Services

2.12.1. Process and Procedures

- Description of solution to meet the requirements

Problem management shall require the investigation of root causes to memorialize occurrences in the Contractor knowledge repository and eliminate future occurrences wherever possible. The process shall also make sure that corrective actions and resolutions are implemented through the appropriate control procedures, such as change and release management. Active incidents and problems shall be documented at every step and the status shall be accessible for End-User review through the Service Portal.

As Contractor has in place today, problem management systems shall also maintain information about problems and the appropriate workarounds and resolutions, so that the organization is able to reduce the number and impact of incidents over time. Although incident management (IM) and problem management are separate processes, they are closely related and typically uses many of the same tools and data points.

Solution: Contractor is assigning a single service delivery manager (SDM) per business group to act as a single point of escalation and communication. Moving forward, Contractor shall take steps that further enhance the ITIL framework, putting more formalization around this process in an effort to continue improvement and to maintain environmental stability.

Problem management shall be under the purview and responsibility of SDMs who shall make sure that all problems are resolved, including root cause determination when necessary. Contractor shall additionally make certain that all problem-related activities be reported and recorded, archived, and made available to County stakeholders.

Rationale:

Problem management shall be a daily responsibility for the SDMs and shall be assigned activities to work—whether it be proactively or through tickets, escalations, or other similar activities. Contractor has an enterprise problem manager who shall report, track, and communicate all problem management issues worked by the team and the account via the weekly CTO operations status meeting.

- Deployment plan for resources and use of facilities

The majority of the services provided by this process are supported by the account team at Contractor's Rancho Bernardo site.

Data center and other areas supported by leveraged frameworks shall provide supplemental support.

The Service Desk provides support from the Pontiac, MI facility.

AT&T provides services from Trade Street site.

- Processes in solution including year-to-year continuous improvement

For Contractor, a problem is any event that has the potential to inhibit the County's ability to perform a business function. Contractor shall provide well-defined processes, key performance indicators, and mature IT tools to alert Contractor's integrated delivery teams when conditions indicate the potential for a problem to occur. Contractor's main goal is to minimize or prevent service degradation to the County's end so the County can continue to perform its duties and service the public unimpeded. Contractor shall train all program team members of these processes, best practices, and lessons learned are shared to maximize effectiveness, promote reuse of knowledge, and optimize project timelines.

Problem Management Techniques and Controls

As a standard practice, Contractor shall conduct enterprise-level delivery reviews weekly to share experiences across the IT services and cross-functional frameworks to identify and mitigate risks.

Recognizing Problems - Contractor uses a methodology-based approach to recognize, address, and correct problems that may arise throughout the IT organization. Contractor's approach combines proven problem management methods and processes, such as root cause analysis, with open communications, transparency, and continuous/iterative feedback. Contractor shall proactively analyze, measure (through leading indicator KPIs), and monitor performance through these multiple channels to increase the probability of identifying and mitigating risks and issues early, before they manifest as incidents or problems.

Correcting Problems – The appropriate SDM shall oversee corrective investigations and problem remediation by designated support representatives. Contractor shall use incident or trouble ticket input as well as procedure manuals, knowledge databases, and other tools to resolve the problem. The SDM shall determine if a workaround can be provided or identify a permanent solution to the problem. Once a workaround or permanent solution is determined, the SDM shall decide on the change needed to implement the workaround or solution. If a Request for Change (RFC) is required, the SDM shall create an RFC. If an RFC is not needed, or after the RFC has been approved, the SDM shall determine whether the implementation of the workaround or solution requires infrastructure support. If needed, the SDM shall create an Infrastructure RFC in Service Desk and link it to the incident.

Resolving Problems among Team Members. If an identified problem threatens the program quality or cost, Contractor shall address the subcontractor directly responsible for the area of nonperformance. In situations where overall contract performance is at risk, Contractor shall issue the subcontractor a written notice specifying the areas of nonperformance.

Subcontractors and the Contractor management team shall meet regularly to discuss overall contract performance. These meetings serve as important forums to identify and resolve potential problems. Open and extensive communication among team members fosters a cooperative atmosphere in which Contractor can jointly resolve problems at an early stage.

Proactive Communications. Contractor's SDM shall maintain transparency with the County through regular communication, reporting on problem progress, and facilitating meetings. The SDM shall be accountable for

maintaining the relationships, monitoring subcontractor performance, identifying training needs, and escalating issues that require higher levels of attention.

Staff, address, and remediate systemic and/or recurring problems.

Contractor shall assign an SDM—and an enterprise problem manager—to be responsible for addressing and remediating systemic/chronic or recurring problems. If necessary, this shall be preceded by an in-depth analysis of an issue such as trends associated with tracking Service Desk tickets. Actions can include the use of Cascade to isolate an issue, or creation of a pan-framework tiger team to address chronic or recurring problems.

Trend analytics to identify and correct recurring problems.

The Contractor enterprise problem manager shall be responsible for analyzing quality and reporting trends. This analysis provides recommendations of appropriate actions to mitigate any negative findings and to propose improvements to drive improved effectiveness and efficiency. As part of the analysis, once a trend is identified, action shall be taken to correct, improve the outcome, or prevent future problems from occurring. Contractor proactive method includes performance-based management and periodic assessments of Contractor's KPIs within the problem management framework. Contractor efforts shall include capturing underperforming mission-critical KPI and SLA metrics, escalating them as necessary, and displaying them on the Enterprise Project Management Office (EPMO) status dashboard. Contractor shall use this data to identify and substantiate trends relating to similar problems or contributing to problem recurrence, and develop solutions to address chronic issues. An integral component of Contractor's continuous improvement process, Contractor continually assesses these indicators to identify negative trends. Contractor shall continue to conduct root-cause analysis where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends; thereby ensuring year-to-year continuous improvement.

Root cause analyses (RCAs) to remediate identified Incidents and Problems.

Contractor shall use problem-oriented RCAs to determine underlying causes, identify appropriate resolutions, document findings, and provide recommendations to prevent recurrence of the problems.

5 Whys and the Fishbone Process

The 5 Whys can be used individually or as a part of the fishbone (also known as the cause and effect or Ishikawa) diagram. The fishbone diagram helps Contractor explore all potential or real causes that result in a single defect or failure. Once all inputs are established on the fishbone, Contractor can use the 5 Whys technique to drill down to the root causes.

Steps to Complete the 5 Whys

- Write down the specific problem. Writing the issue helps you formalize the problem and describe it completely. It also helps a team focus on the same problem.
- Ask why the problem happens and write the answer down below the problem.
- If the answer you just provided doesn't identify the root cause of the problem that you wrote down in Step 1, ask why again and write that answer down.
- Loop back to Step 3 until the team is in agreement that the problem's root cause is identified. Again, this may take fewer or more times than five Whys.

2.13. Change Management Services

2.13.1. Process and Procedures

- Solution to meet the requirements and the rationale

The change management process itself is the sequence of steps or activities required to implement County-approved changes into the environment and verify the outcomes are as intended. ITIL methodology is the foundation that Contractor shall provide for change management. Overall, Contractor is an advocate and champion of successful change management as an integral component of Contractor's cross-functional management processes and best practices.

Solution: The foundation of Contractor's change management approach shall be its ITIL certified processes, of which change management is an integral component. A key element of the approach shall be assigning a single service delivery manager (SDM) per business group to act as a point person and to monitor changes that may impact that space. SDMs shall be responsible for making sure that proper communication and discussions for that framework take place and that resources are available to support the RFC owner for testing/validation.

- Deployment plan for resources and use of facilities

Operating out of its Rancho Bernardo facility, the Contractor Change Manager shall implement and sustain repeatable, methodically driven change management processes and best practices. Timely, accurate, available stakeholder documentation is an integral part of the change manager's activities, which Contractor shall coordinate with County counterparts.

- Key methodologies and processes in solution including year-to-year continuous improvement

The Contractor IT Change Management Suite and Services shall support multiple types of change requests and mitigate the risks associated with potential requests. The Change Management Suite shall integrate change processes into the broader ecosystem in a cost-effective way, providing full and open transparency and progress reporting. Contractor's Change Management Suite tool shall assist in the continuous improvement needed in this framework, shall greatly enhance configuration visibility and stability, as well as monitoring the type and frequency of upgrades that may be required.

Contractor IT Change Management shall be part of an integrated set of ITSM process modules for Service Manager.

The Contractor IT Change Management Suite shall come with embedded, out-of-the-box IT Infrastructure Library (ITIL)-based best practices. It shall create mechanisms for measuring change process workflows, automate impact analysis, and enhance Change Request Control Board (CRCB) virtualization. Additional efficiencies include reduction in total time needed to process changes, a benefit provided by enabling the changing of approvers via smart phone. This feature shall facilitate approval of changes anytime, anywhere.

The Contractor IT Change Management Suite shall provide the County the option to create standardized and repeatable workflows. The suite shall include built-in best practices with associated industry-standard workflows, forms, and documentation. The suite shall create, modify, and reuse change processes, enabling continuous service improvements. With the Contractor IT Change Management Suite, different change types shall follow different paths. Pre-approved changes for standard requests shall be expedited while others follow a normal/conventional completion process. Scriptable and repeatable processes, including release management, provide the foundation for reducing risk and enhancing the benefits associated with change.

To help County visualize the end-to-end process, the Contractor IT Change Management solution shall provide a graphical workflow interface. The County shall be able to design, modify, and visually monitor multi-level

processes. The solution shall expose every element of a change process—people, assets, timeframes, tasks, phases, and notifications—in clear, visual terms.

Through the Contractor IT Change Management Suite, the County shall be able to coordinate change activities across users and CRCB members, decision-makers, and other stakeholders involved with the change process. The County shall also be able to enable the suite to send automatic notifications to parties regarding potential changes affecting their respective systems.

The County shall additionally be able to assign, execute, and track CRCB action items, discussion threads, impact assessments, and voting. The Contractor IT Change Management Suite shall also automate potential collision detection, impact analysis, and risk assessments of change to the business. Moreover, the County shall be able to virtualize CRCB functions to enable decisions outside of actual meetings, increasing meeting effectiveness.

The Suite shall also include a global forward schedule of change that brings change requests together into a unified common view, providing improved visibility and planning. Change calendars shall be based on multiple views—including an Outlook-style calendar with timelines by month/week/day/hour, by application, and by implementer. This feature shall provide insight into the impacts, collisions, and comments of every change request. In addition, the Contractor IT Change Management Suite shall assign and track change windows, freeze periods, and business events, giving the County better control over when changes are implemented.

Contractor Service Manager solution and the Contractor IT Change Management Suite shall share configuration and dependency information found in an ITIL-aligned configuration management system (CMS) built on the Contractor's Universal Configuration Management Database (uCMDB). The Suite shall automatically and continually perform impact analysis, risk assessment, and collision detection on all change requests. Impacts and collisions shall be based on infrastructure and application relationships, but they can also reflect timing conflicts in personnel schedules (for example, the people responsible for implementing changes).

The Suite shall flag all impacted configuration items, potential applications, and associated business services using dependency mapping information. It shall also compare new change requests to all other pending requests within the same timeframe, and shall identify potential collisions that could result in downtime and rework. The Suite shall calculate a score based on multiple criteria—including historical outcomes of similar changes—for more accurate risk assessment.

As part of the overall Contractor's Service Manager solution, the Contractor IT Change Management Suite shall be tightly integrated with other ITSM processes and modules—from the logging of change requests through implementation, evaluation, and closure. This shall include integration with catalog, request, incident, problem, configuration, and service-level management components of Contractor Service Manager.

The companion Service Manager Service Catalog and Request Management modules shall provide integrated front ends into the change process.

Contractor Service Manager shall provide dashboards and reports that shall be easily customizable to provide managers and County leaders with quick and concise views into the overall status of the change process while enabling drill-down access to more detailed information.

The complete change process—from assembling requests through implementation and execution of change—shall be automated to speed the delivery time for standard change requests. Contractor shall integrate Contractor Operations Orchestration to enable faster RFC creation, change execution and provisioning, and closed-loop validation.

The Contractor Service Manager knows the "managed" state of configuration items (CIs)—or the state in which a CI is expected to be. The Contractor Universal CMDB with discovery and dependency mapping information shall maintain the "actual" states. After a change has been implemented, the managed and actual states shall be compared to validate that a change was successfully completed. In a similar manner, when a configuration item

changes, the Contractor IT Change Management Suite shall compare this actual state of a CI against the record of change requests. Any change that does not have a corresponding change record shall be identified and addressed appropriately—by methods such as creating an incident or a new RFC.

The Contractor IT Change Management Suite shall enable Contractor and the County to establish effective IT process controls for change and configuration management. The built-in best practices based on ITIL shall align with common auditing frameworks such as Control Objectives for Information and related Technology (COBIT).

County involvement in the Change Management process.

All changes shall go through a formal change approval process as follows:

- When a change is desired, the change initiator shall complete an RFC ticket.
- The RFC shall be reviewed in the internal Technical Approval Board (TAB) review before it is released to County stakeholders.
- The RFC is submitted to the CRCB, which consists of both Contractor subject matter experts (SMEs) and County CTO representatives.
- The CRCB shall review the RFC and approve or disapprove the change.
- If the change is approved, the change initiator shall be notified as well as County end-users, and a Change Release shall be initiated.
- The Change Release shall be monitored through implementation and closure.
- A Post Implementation Review (PIR) shall be completed for each change at the completion of the RFC.

Metrics to measure the effectiveness of changes and conduct continuous improvement of the change management process.

Contractor shall continually assess these KPIs to identify negative trend lines. Contractor shall conduct root-cause analysis where necessary and take appropriate remediation steps to improve the KPIs and positively influence performance trends, thereby facilitating year-to-year continuous improvement.

2.14. Release Management Services

2.14.1. Process and Procedures

- Description of solution to meet the requirements

In practicing release management, Contractor shall combine the general business emphasis of traditional project management with a detailed technical knowledge of the system development lifecycle (SDLC) and ITIL practices. Contractor shall operate release management services in accordance with these practices, in complete transparency and collaboration with County stakeholders.

Solution: While the enterprise release manager on the account shall be responsible for tracking and logging all releases, the SDM for each business group shall perform this critical role. The SDM shall be responsible for understanding, monitoring, and assisting in the communication of these releases as they are completed in their respective business group.

In addition to the release review meeting that the release manager shall hold with the Contractor and County stakeholders, releases shall be reported in regularly scheduled meetings that the SDM shall be required to attend that fall within the scope of their duties. The SDM shall understand all information related to releases affecting their respective business group, bringing in SMEs if additional information is required.

Release management shall fall under the governance of the CRCB, which shall consist of both Contractor SMEs and County CTO representatives. All configuration items distributed into production shall use a formal release management process. Contractor shall develop a Release Plan that outlines the release schedule, content of the release, and back-out plans. Release management shall work with configuration management to make certain that the Definitive Software Library master IT configuration items remain current.

Rationale: The enterprise release manager shall be responsible for continuous improvement and shall work in collaboration with the County to facilitate the continued effectiveness of the process. Contractor's SDMs shall be responsible for understanding the releases and how they impact their respective business group. Contractor release managers shall be responsible for providing adherence to SDLC, ITIL, and Contractor best practices. They shall verify the completed release process is thoroughly documented and communicated to County stakeholders.

- Deployment plan for resources and use of facilities

The enterprise release manager shall work out of Contractor's Rancho Bernardo site.

- Key methodologies and processes in solution including year-to-year continuous improvement

The accuracy and diligence that Contractor provides in software configuration management (SCM) shall be realized by relatively issue-free releases, as Contractor moves into production and provide a stable, sustainable, and predictable release.

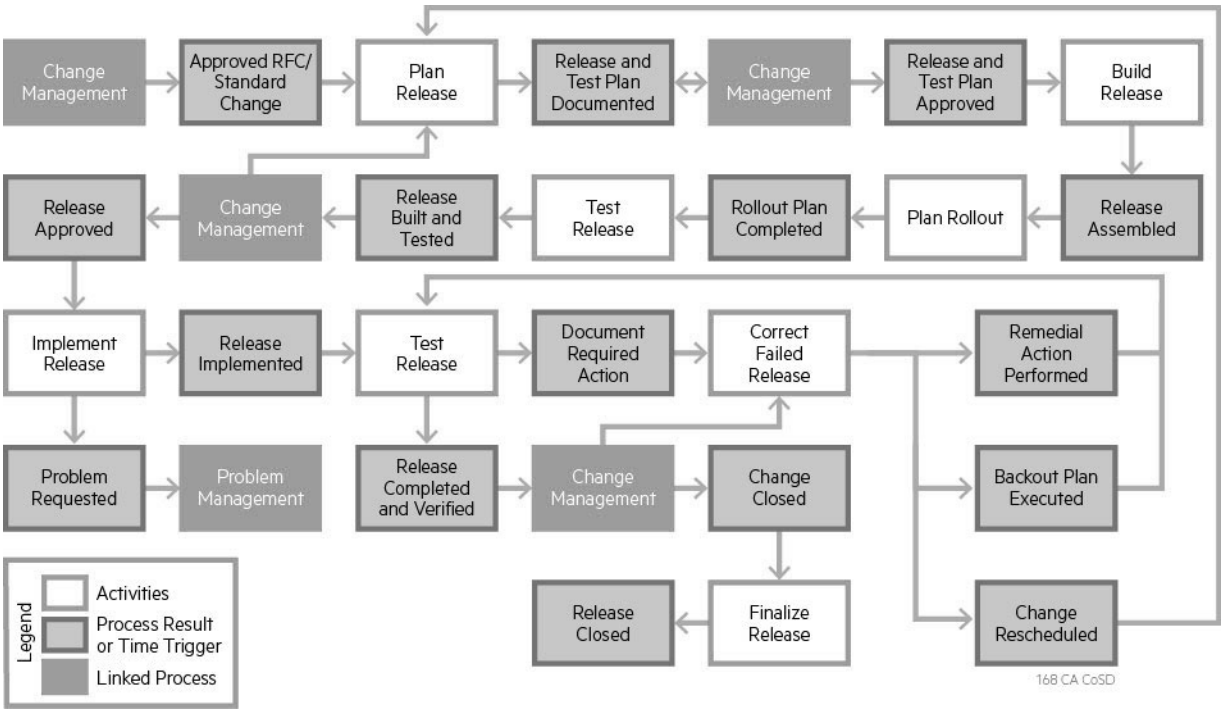
Release management is the process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. Its primary objective is to protect the integrity of the live environment and to make sure that the correct components are released.

Deployment is the activity responsible for movement of new or changed hardware, software, documentation, and processes to the live environment. The term "rollout" is most often used to refer to complex or phased deployments or deployments to multiple locations. Specific objectives of the process shall be as follows:

- Aligning, coordinating, and communicating release and deployment plans with County projects.
- Successfully building, installing, testing, and deploying a release package to the target environment along with the necessary documentation and training.
- Making certain that the new or changed service and underlying infrastructure are delivered to the agreed service level, providing the service utility, warranty, and level.
- Keeping to a minimum the impact on production services, operations, and support staff and business in general.

The following figure illustrates the Contractor standard release process.

Contractor Release Management Process



Proven process makes sure changes are effectively communicated, properly tested, and configuration controlled.

Contractor shall bring the change management process and shall align with and embrace the County's release management policy.

2.15. Configuration Management Services

2.15.1. Process and Procedures

- Solution to meet the requirements

Configuration Management (CM) is the detailed recording and updating of information that describes an organization's hardware and software. The tools are as follows:

- Apps Manager – Application related information
- Enterprise Server List (ESL) – data center hardware information (severs/storage/network/etc.)
- Asset Manager – Desktop-related asset information
- Endevor – Mainframe
- Serena – Archived source code related to applications
- Team Foundation Server (TFS) –Current source code solution
- AT&T data

Contractor shall adhere to the current Contractor-provided Configuration Management Plan, which supports/requires close customer collaboration and governs Contractor's activities related to CM.

Solution: Contractor shall provide a Configuration Management System (CMS) and multiple CMDBs, accessible through the Service Portal that supports activities associated with recording, tracking, updating, and disseminating the County's configurations for all assets, including network assets. The CMS integrated across the organization and service frameworks shall support all logical configurations of hardware and software for the services. The CMS contains mappings to physical configuration, inventory data of hardware and software; Contractor shall use it to analyze trends as well as manage and reduce incidents and problems. The Service Portal shall display all information related to all assets from each tool mentioned above.

Contractor shall continue to provide software configuration management (SCM) via Apps Manager for the County of San Diego portfolio applications. Contractor shall make available the version control history as well as current versions of portfolio code and artifacts, including application code, software tools, and artifacts. Application SCM is part of the program CM and conforms to those policies and procedures.

Discrete item identifiers shall be associated with all configuration items (CIs). Applications' CIs include source code, compiled and/or linked code, packaged code, development environment tools, and any related documentation such as End-User manuals, test scripts, test results, project management documentation, architectural drawings, run books, and helpdesk scripts. Contractor SCM shall provide physical and logical online libraries for the CM of all software CIs. Contractor shall provide hardware-related information from ESL, which is where data center related equipment is tracked and controlled, and Asset Manager, which includes desktop-related hardware items. Contractor SCM is integrated with hardware configuration management data via a feed from ESL to Apps Manager.

Contractor SCM shall provide three libraries for applications code: two based on platform and one for vendor-delivered media. While Mainframe code resides in the legacy Endevor library on the mainframe, Windows and midrange code reside in TFS. More than a version control system, TFS uses a SQL Server database as a means of scaling to large environments and infrastructures. TFS shall be the key component in the life cycle platform, which enables third parties, customers, and solution providers to extend the base functionality with new features and customize the tool for unique County requirements and initiatives.

Contractor SCM shall manage third-party vendor code to include contracted code, public domain, purchased, and commercial off-the-shelf (COTS) packages. Third-party vendors shall use TFS for development of all applications CIs, unless a program-approved provision is in place for offsite development for that application. Third-party vendors shall make certain all code and artifacts are delivered in accordance with the Agreement. Contractor SCM shall review the third-party SCM practices and place the vendor deliverables under configuration management for the program.

Contractor and County-contracted third-party vendor code developed or maintained offsite shall follow County security and Contractor SCM standards. Purchased, public domain, and COTS software packages shall be implemented following County security requirements.

Rationale: Contractor's cross-functional configuration managers shall be responsible for understanding the interrelated and complementary CM requirements and best practices, and how they impact different frameworks and the greater IT organization. Cross-functional configuration managers shall be additionally responsible for making sure that proper communication and discussions for framework take place and that resources are available to manage and support all CM activities including reporting and portal accessibility by County stakeholders.

- Deployment plan for resources and use of facilities

CM personnel shall operate out of the Contractor's facility in Rancho Bernardo. AT&T personnel shall operate out of their facility on Trade Street.

- Key methodologies and processes in solution including year-to-year continuous improvement

Central to IT Service Management is a CMS and a set of core Service Management tools and databases that provide data to other ITIL or IT Service Management processes to deliver and support IT services throughout the County. The CMS comprises one or more CMDBs that collect and consolidate data from multiple sources into an aggregated view critical for timely and accurate decision-making.

TFS, for example, is a commercial software product specifically designed for CM administration that has been deployed at the County. All types of events that result in software or environment configuration changes shall be documented and tracked from initiation to closure.

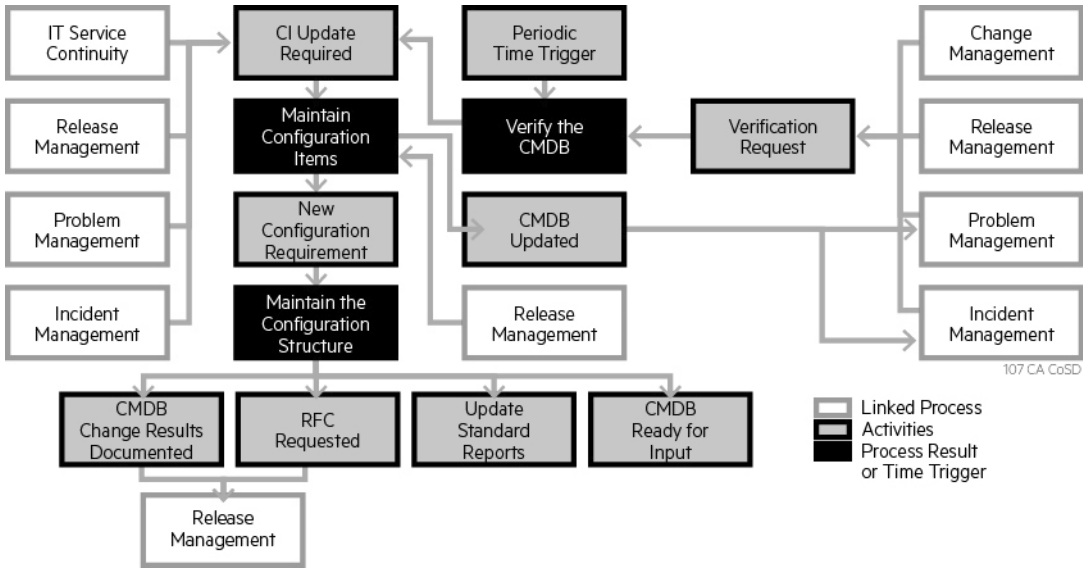
The primary purpose of CM at the County shall be to make certain that product attributes and technical baselines of all software and systems in use by the County—collectively known as configuration items (CIs)—conform to the documented design for each released software version. This shall include the means to document, track, and audit all design decisions and design modifications as well as software and environment build processes that verify the as-built software and host environments exactly match the intended design. CM is an activity that spans many groups across the organization, including management, requirements, process controls, tracking data, development, software tools, archival records, audits, and testing.

County CM shall include two primary teams that handle the bulk of the day-to-day CM tasks. Contractor shall perform this function and is primarily responsible for verifying that development proceeds according to the organization's documented CM rules. This group, with responsibility for the customized controls and rules, shall document and implement CM processes in a manner that is visible to all personnel; this group shall also make certain that released versions of County software products match the required and scoped content planned for that release. This group shall handle most CM status accounting functions and audit report functions, which are heavily automated through TFS. The second group is a development support team, whose duties shall include maintaining a fully versioned source code repository for each of the major County systems; developing automated build processes; building automatic installation packages; and providing software deployment across development, test, and production environments.

All modifications to this plan must obtain signoff by the County before going into effect. Additionally, quarterly quality reviews shall be conducted on the enterprise CM process, and results shall be reported to the County. Process End-User feedback and technology enhancement shall be used to continually improve the process.

The following figure depicts Contractor's standard CM process.

Figure 1. Contractor's Standard Configuration Management Process



Delivering quality ITIL-based CM processes that the accuracy, currency and visibility of CIs

Solution for the integrated configuration management database that covers all Service Frameworks.

Contractor's integrated CMDB shall record various CIs along with their attributes and relationships on behalf of the cross-functional service frameworks. Comprised of various framework CMDBs, the integrated CMDB and View shall be organized by framework and other key attributes. This shall enable individual CMDB CM administration as well as composite or service-wide CM. The Contractor configuration manager shall be responsible for the integrated databases.

Processes to maintain currency and accuracy of the integrated CMDB.

Contractor shall deploy auto-discovery tools to maintain accurate and current CMDB CI information.

Contractor shall proactively engage at all levels to make sure that the IT services it provides and sustains are optimal to meet the County's current and evolving needs. Contractor shall collaborate with the County to provide and respond to the "over-the-horizon" view, which shall include at a minimum vigilantly monitoring asset inventories and software upgrades. Contractor shall make sure all iterations are captured and stored in CMDB and that County stakeholders are made aware of any anomalies or issues.

2.16. Capacity Planning and Performance Management Services

2.16.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor's capacity planning and performance analysts shall collaborate with appropriate stakeholders in determining the resources required and make sure the performance or availability constraints shall not

adversely affect County business. Response times and quality of services for End-Users shall be used as input and relevant data points to these decisions and performance assessments.

Contractor shall provide hardware, software, and configuration updates to servers, storage, desktops, and network so that the capacity maintenance and management is performed. The process shall involve the assembly of accurate reports of shortfalls, analysis of those shortfalls, and development of a solution to solve any capacity items that do not meet the goal. Contractor shall employ a cross framework process for ongoing proactive anomaly detection that involves representatives from all frameworks. The solution shall be implemented using existing data center procedures that may include County change approval. Virtual server implementation requires reconfiguration and can be done quickly, while implementation of physical servers may require the installation of new hardware, software, and/or configuration items. Changes recommended and approved shall be processed through the change process for implementation. After implementation, the responsible framework shall verify the effectiveness of the solution.

Contractor shall develop the Annual Capacity Management Procedures (ACP) as a key component of the Contractor solution. The purpose of ACP shall be to forecast County IT capacity and performance requirements on an annual basis and reaching forward. The ACP shall balance needs over the long term to optimize the resource workload expected in coming years. The primary inputs to the ACP process shall be historical performance information during the past year and the CTO technical roadmap, so that the forecast encompasses all data needed to meet immediate and extended future capacities and all service levels.

The output from this process shall be the projections for the next 2 years of IT capacity necessary to support the forecast, including identification of OS upgrades required to support the forecasted capacity.

The initiation of the ACP for report delivery to the County for review and approval shall begin during the mid-October timeframe.

The cross-functional capacity and performance management process shall assemble the prior year's historical information, including business forecasts, and shall generate the forecast during the planning period, including identifying OS upgrades if required.

The ACP shall be used to tune the performance management process for the new workload, and to selectively identify problems/opportunities that are to be undertaken as projects to mitigate some of the workload. The performance management process shall collect current system capacity and/or performance data and perform predictive analysis to identify the current capacity limits. This data shall be stored and used in annual capacity planning as historical information.

New desktop hardware technology shall be reviewed annually by desktop engineering. Capacity and performance specifications for desktop hardware and desktop applications in use or planned shall be reviewed with vendors to accommodate current and future County requirements and expectations. A report of recommendations shall be presented and reviewed with the CTO. The information collected throughout the year shall be incorporated into the ACP, providing adequate desktop services to maintain service delivery.

Rationale: Contractor's capacity planning and performance analysts shall be responsible for understanding the interrelated and complementary requirements, and how they impact different frameworks and the greater IT organization. In addition to discovering and analyzing critical touch points and KPIs, Contractor analysts shall thoroughly document and report their findings and activities and make the information available to County End-Users through the Service Portal.

- Deployment plan for resources and use of facilities

The positions required to provide capacity planning and performance management services are capacity planning manager and IT capacity planner. These personnel shall reside in Contractor's Rancho Bernardo facility. Network capacity planning shall be augmented by AT&T operating out of its facility on Trade Street.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor capacity management shall be an ITIL-compliant service that helps prevent business disruptions by proactively managing system use and capacity.

Contractor shall proactively and continually monitor capacity so that availability does not fall below 75% and potentially result in degraded performance and a net-negative impact to the business. Contractor shall also monitor and identify capacity usage, possibly indicating architecture design or program configuration anomalies.

Capacity management shall make sure the County IT infrastructure is ready to meet the demands of users at agreed operational levels today and that IT services have the capacity to support future requirements. This shall be accomplished through collecting, analyzing, and reporting on capacity statistics and assessing the impact of County-planned projects. Contractor shall work closely with County to plan and budget IT capacity based on changing business requirements, as well as recommend improvements for optimization of infrastructure investments.

Contractor shall provide the County with data collected through automated reporting with an analysis of in-scope components' capacity consumption. A collection of reports shall display standard component utilization metrics, such as memory and CPU capacity.

Contractor shall group, and trend by day, all data for a single calendar month or monthly for the past 12 months.

County employees with access to the Service Portal shall be able to view the capacity reports at will, giving them the freedom to access data and reports as required. County employees shall be able to export reports to Adobe Acrobat, MS Excel, MS Word, or Rich Text format, enabling further analysis, combining with other data, or including in presentations and other documents.

Using automated scripts, Contractor shall extract use data monthly from data collection servers and load it into the capacity management application. On a monthly basis, Contractor shall produce a forecast report using historical data that is trended over 12 months. Graphs include installed, usable, and forecast capacity data points.

The capacity management process shall rely on the key concept of a capacity management plan, which is a calendar-based data store that keeps track of workload identities, forecasts, and resource access quality of service requirements; resources that are associated with a pool; and assignments of workloads to resources. As a calendar-based data store, the plan shall keep track of such information as a function of date and time and uses it to support capacity planning.

"Configure resource pool size" shall be used to reduce capacity fragmentation by periodically repacking or consolidating workloads in a pool. "Find placement" shall balance loads, dividing them evenly across resources. It has two stages—if no resource is able to support the resulting capacity requirements, then Contractor shall attempt a larger scale rebalancing of workloads, adjust workload quality of service requirements, or combine the two approaches. "Add workload" shall report whether a placement can be found for a new workload.

Monitor, analyze and optimize capacity and performance in a virtualized data center.

Contractor shall provide capacity planning and performance optimizations as follows:

- Virtualization involves a different level of abstraction, where the relationship between shared resources is in a constant state of flux. Although enterprises view the supply side of capacity planning as pools or clusters of virtual resources, they must also understand which cluster or pool to use for an application and the broad impact on a virtual environment. For example, Contractor's virtualization specialists shall determine which clusters or pools need more resources as well as how updating virtual resources affects other resources. They shall make recommendations on how to deal with virtual machine (VM) sprawl (a proliferation problem), and when to reduce VM resources if Contractor believes they may be needed soon, but not currently.

- Although capacity planners have always been concerned about waste (or how much oversupply to have in reserve), the concept takes on new meaning in virtual environments, where the ease with which VMs and applications can be created has led to VM sprawl. Depending on the environment, waste due to VM sprawl can be considerable. Without proper insight into consumption requirements, enterprises risk vastly overestimating the resources needed to support their virtual environment.
- VMs do not exist in isolation; they run complex (often multi-tiered) applications that support many lines of business. Being able to profile how applications and business departments use (or potentially waste) the underlying physical resources is key. Even without a formal chargeback process, organizations need to understand how resources are being consumed so budget considerations can be calculated and sensible use of resources can be encouraged to meet demand.

Contractor VM specialists are experienced in VM environments and demand nuances, and share this experience and expertise with Contractor's capacity planning and performance analysts to make sure County virtual environments are accurately planned, used, and measured. Contractor shall proactively and continuously monitor capacity so that availability in the virtual environment does not fall below 75% and potentially result in degraded performance and a net-negative impact to the business. Contractor shall also monitor and identify capacity usage, possibly indicating architecture design or program configuration anomalies. Should virtual capacity or performance require additional resources, Contractor shall immediately substantiate and initiate appropriate requests and notify appropriate stakeholders.

Once virtual environment considerations are factored in to the demand and use parameters of capacity planning and performance optimization, normal activities shall make sure the following occurs:

- Contractor shall use an ITIL-compliance capacity management service that helps prevent business disruptions by proactively managing system use and capacity. Making sure the right capacity is always available can mean increasing capacity based on County business and IT needs, or reducing or reallocating capacity so the County pays only for the hardware, software, and support needed.
- Capacity discovery shall occur through collecting, analyzing, and reporting on capacity statistics and assessing the impact of the County's planned projects. Contractor shall work closely with the County to plan and budget IT capacity based on changing business requirements, as well as recommend improvements for optimization of County's infrastructure investments, including people, processes, and tools.
  - Contractor shall extend this environment with sufficient capacity to accommodate increased workloads to include a new purpose-built Managed Private Cloud (MPC) environment. The MPC environment shall be a highly standardized environment with high-redundancy and scalability.
- Utilization reporting shall use data collected through automated reporting to provide an ongoing understanding and analysis of in-scope components' capacity consumption. A collection of reports shall display standard component utilization metrics, such as memory and CPU capacity. The lowest level of detail shall help with capacity planning and management.
- The capacity trend reporting feature shall provide more advanced reporting capabilities than the standard use report. Using automated scripts, Contractor shall extract use data monthly from data collection servers and load it into the capacity management application. On a monthly basis, Contractor shall produce a forecast report using historical data that is trended over 12 months. Graphs shall include installed, usable, and forecast capacity data points.

- Use of Tools

The automated tool Contractor shall use to provide capacity planning is Contractor's Global Delivery Capacity and Performance Management (GDCPM) tool. This is a data warehouse that shall include database, storage, telecom, and networks. Other types of infrastructure data include system/server capacity management (forecasting and trending) metrics, availability metrics, and Performance management data.

2.17. Disaster Recovery Management Services

2.17.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor's DR management services shall provide strategy, process, type, methodology, locations, documentation, and prompt restoration of services. Contractor's solution is a subscription model, based on the County's specified Recovery Time Objective (RTO) and Recovery Point Objectives (RPO). Applications with a 72-hour RTO shall be recovered from replicated Virtual Tape Library (VTL) backups. Applications with a 48-hour RTO shall have their DR servers mounted to a replicated SAN storage. Under a subscription model, the server hardware "subscribed" to by the County is leveraged, provisioned with County images and applications on an as-needed basis to support DR tests, or actual disaster events. However, if shorter recovery times are required in the future, Contractor can implement active/active and/or active/passive-solutions, using dedicated server hardware, for web, application, and data layer recovery. License costs for active/active-synchronous, active/passive-asynchronous and active/passive vault tools are not included in base services.

During transition, Contractor shall validate ongoing DR policies and procedures including:

- Portfolio application priorities and Recovery Time Objectives/Recovery Point Objectives (RTO/RPO) requirements including:
  - Validation that restoration times meets County requirements
  - The server strategy (subscription using replicated backups or SAN data, or one of the dedicated hardware options above)
  - Data synchronization and replication plans
  - Rationalization of licensing costs.

The DR environments for the virtual servers within the MPC shall be virtual servers that spin up with a copy of the MPC virtual server.

Contractor's solution is based on F5 Global Traffic Manager (GTM) and Akamai. In in the event active/active, is implemented, Contractor shall support a synchronization technology such as SQL server Always-on architecture and Oracle Data Guard architecture. Contractor's technology Continuity of Operations (COOP) professionals, whose primary mission is to build a robust DR program for the County, shall write a viable and executable DR plan and schedule and manage DR exercises. Upon declaration of a DR event, Contractor shall execute the County Disaster Recovery Plan (to be developed during transition) that shall include:

Recovering and resuming full operations including all supporting infrastructure and networks in accordance with SLAs.

Rationale: Contractor's enterprise service delivery manager shall be the County point person and the conduit for information flow between remote disaster recovery managers and the County. Contractor's enterprise service delivery manager (ESDM) and remote DR managers shall be responsible for communication, managing resources, and supporting all DR activities, including during and after the event, which shall include a complete report to the County.

- Deployment plan for resources and use of facilities

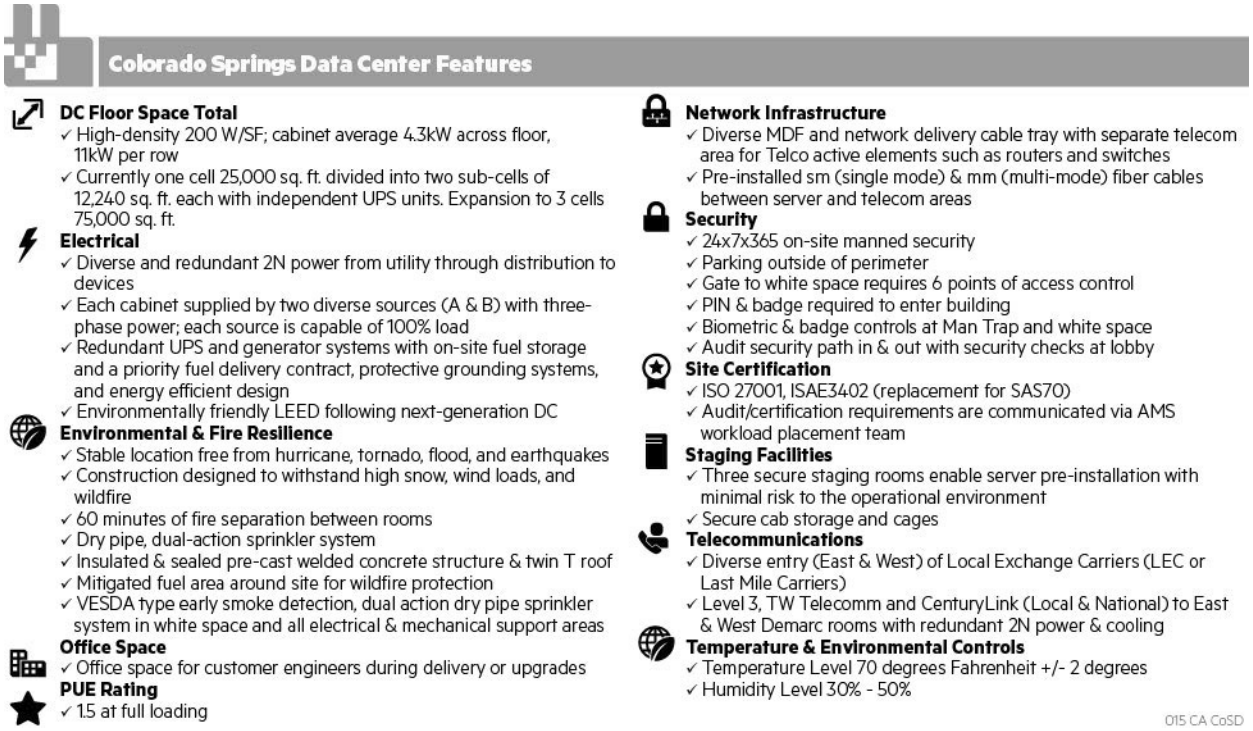
The County's recovery site shall be Contractor's Colorado Springs, CO Data Center (CSDC), connected via dedicated 10GB circuit, providing data replication. Contractor shall be able to provide a wide variety of disaster recovery services—dedicated to shared and/or hybrid solutions—at this central location.

Contractor shall write, maintain, and exercise County DR plans, and data center management professionals shall maintain the hardware, replication, and synchronization aspects of the solution. Connectivity and synchronization with CSDC shall include HPE's Tulsa production/development center and the County operations data center, as well as the AT&T POP, DR POP, Tower 9, Lemon Grove, and future sites as required. Coordination shall be managed by the Contractor ESDM.

The CSDC shall be a purpose-built, SSAE16-audited, data center. The Tier III data center design shall provide a completely redundant and continuously operating facility with infrastructure built with hot-swappable components, redundant power supplies and fans, compact flash, multi-boot support, and always-on management. Data synchronization and replication shall be determined by each application's RTO and RPO, and VM server versus physical server recovery methodology. Appliances shall be able to be deployed in traditional active/standby configuration or horizontal clusters (active/active) to achieve high availability and application-level failover. Contractor's CSDC MDRS facilities shall include locking cages, cabinets, and racks to meet County physical security requirements. This facility shall be used to provide DR and data backup services for Contractor's USPS clients as well as HPES Corporate.

Access to the CSDC shall be highly restricted. Access to network and Contractor computer equipment, storage media, critical support areas, and operations documentation shall only be granted to authorized personnel. Security consoles linked to alarm systems and closed circuit TV (CCTV) cameras shall be manned. Security cardkey readers shall protect all doors leading into the data center, and issuance of cardkeys for physical access to the facilities shall be controlled through a request and approval process. The following depicts features and capabilities of the CSDC.

CSDC Features and Capabilities



Providing comprehensive, full-service data center capabilities that facilitate continuous processing and operational stability.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's DR program shall be built on industry best practices and standards of the Disaster Recovery Institute International (DRII) and ITIL. This model shall define four phases in the DR life cycle of a business continuity program—Analysis, design, build and integrate, and manage and evolve. The DR program shall include periodic and short-notice drills to validate the processes.

This model shall be flexible and adaptable, enabling phased implementation for the overall continuity program and for the County to enter and exit the life cycle at any point within the methodology process path.

The design phase is an enhanced DR (EDR) solution and the subscription DR solution for the 48- and 72-hour RTO systems respectively.

Contractor's delivery team shall start with the build and integrate phase and stand-up the DR environment while Contractor continuity professionals begin the preliminary stages of drafting the DR plan. In this phase Contractor shall provision the replication circuit between the Tulsa data center and the CSDC recovery site. Contractor shall verify that data replication is occurring accurately and as planned. At the end of the phase, Contractor shall perform a tabletop exercise of the DR plan to validate its functionality and address any deficiencies found during the exercise.

At the conclusion of the tabletop exercise, the management and evolution phase of the DR program life cycle shall begin. In this phase Contractor and shall create and provide a master DR exercise calendar for County approval and work closely with the County to reflect the production changes into the DR environment in a methodical and timely manner. Contractor shall provide required training during this phase to make sure it is operating as expected.

In the analysis phase, Contractor shall work with County and assist in yearly undertakings such as a Business Impact Analysis (BIA) or identification of critical systems and apps. The following table outlines the features and benefits of Contractor's approach.

Critical System Features

FEATURES	BENEFITS
CSDC Tier III, HPE corporate DR services, Federal DR clients, and is highly redundant and secure	• Highly skilled and experienced engineering, operations, security and program management resources • Experienced testing and compliance personnel
Network design that is redundant and secure, with automated GTM and load balancing capabilities with multi-layered firewall design	• Uses the skills and experience of Contractor's network operations personnel • GTM automation works to reroute IP traffic in the event of a declaration • Automatic and transparent recovery and continuity of service

FEATURES	BENEFITS
Automated, continuous host-based replication for 48-hour RTO systems	• Automated, real-time maintenance of host images and data integrity • Near real-time RPOs • Can failover or fall back virtual-to-virtual or physical-to-virtual systems
Industry recognized DR PLANNING leader (Forrester-Traditional Disaster Recovery Service Providers)	• Highly skilled, trained, and BCM-certified personnel • Comprehensive development methodology • Experienced with Federal standards including NIST SP 800-34 Rev. 1
Continuous Process Improvement Loop	• Independent monitoring during exercises followed by after-action lessons learned to identify and integrate ways to improve DR processing

The DR plan shall be a cohesive document that includes an auditable overview, team structures, responsibilities, contact information, detailed recovery procedures, and recovery site activation aligned with NIST SP 800-34 Rev. Developed using Contractor templates, the plans shall be stored in a secure area of the Service Portal with access to authorized personnel only. Contractor shall design the plans to enable hand-off to County staff to complete its portion of the recovery and for data validation. Contractor shall also work with the County to create disaster definition and declaration processes relative to this proposal.

After approval, the DR plan shall be reviewed during an initial tabletop exercise. This exercise shall be conducted with County staff and operational leaders to fine-tune plan details and serve as a means to provide initial training to the County and Contractor. Additional training shall be provided to the County and Contractor delivery team as requested by the County.

As a standard operating procedure, Contractor shall incorporate client change management processes into the DR life cycle. Any change to the production environment shall be captured in the DR plan and the MDRS environment or it becomes impossible to maintain a viable and executable plan. Therefore, Contractor's lead continuity professional on the account shall be a member of the change control board.

Annual DR Exercises

Contractor shall schedule, plan, and lead one DR exercise annually in cooperation with the County. Contractor shall create and provide for County approval the strategy for the testing scope and a master schedule. Depending on various elements such as impact to the production environment or availability of the resources, exercises shall be live or table-top exercises. When possible, a DR exercise shall include an entire IT production site, or exercises shall be for all the applications in a given recovery tier or for a logical grouping of the applications. Contractor shall coordinate the following items:

- Laying out the entire exercise process with specific milestones, objectives, and metrics for each scheduled exercise
- Putting measures in place that track objectives

- Coordinating and preparing with the County application teams, users if desired, and any third-party vendors required
- During the exercise, measuring and tracking recovery timelines according to the County's RTOs and RPOs
- Documenting exercise results in a formal report, including comparison of the results to the measures and goals established, action items from the exercise, and recommendations on how the recovery process could be improved to be faster and more reliable
- Updates to plans as needed

County involvement with the Disaster Recovery plan.

County shall:
- Define RTO requirements
- Review/approve or disapprove DR plan
- Participate in drills and tests.

County Data recovery and restoration to meet the Service Levels.

For County data repositories restoration with no greater than a 28-hour data loss, Contractor shall provide data synchronization and replication that includes the County's immutable storage, live data, and virtual tape libraries.

For the systems and applications with a 48-hour RTO, Contractor shall use Contractor's EDR. This solution, which shall consist of replicating data center data asynchronously between the Tulsa production site and the CSDC recovery site, shall meet RTOs in as short as 4 hours.

For the systems and applications with a 72-hour RTO, Contractor shall:

- Deploy virtual tape libraries between the production and recovery sites, using the same replication circuit provisioned for EDR above. Contractor shall subscribe to physical or virtual servers for DR tests or during a true disaster event. Contractor continuity professionals shall stand up these servers within 12 hours of the disaster declaration, leaving 60 hours of the balance of the RTO to reconstitute the applications and data on the servers.

2.18. Identity Access Management Services

2.18.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall use IDAM technology to initiate, capture, record, and manage End-User identities and their related access permissions. Contractor shall make certain that access privileges are granted according to a singular interpretation of policy and that all individuals and services are properly authenticated, authorized, and audited.

Contractor's approach to provide IAM Services for the County shall be to:

- Enable the County to continue to execute its Identity Management Road Map
- Minimize risk and cost to the County by leveraging the County's current investment in Oracle IDAM platforms
- Build on the current Active Directory and Active Directory Federation Services (ADFS)
- Build on current PKI solution

All production servers, production storage, and Oracle licenses for the IDAM platform shall be provided through the applicable resource units and Third-Party Services.

The following table summarizes the billing approach for Identity Access Management Services (IAM):

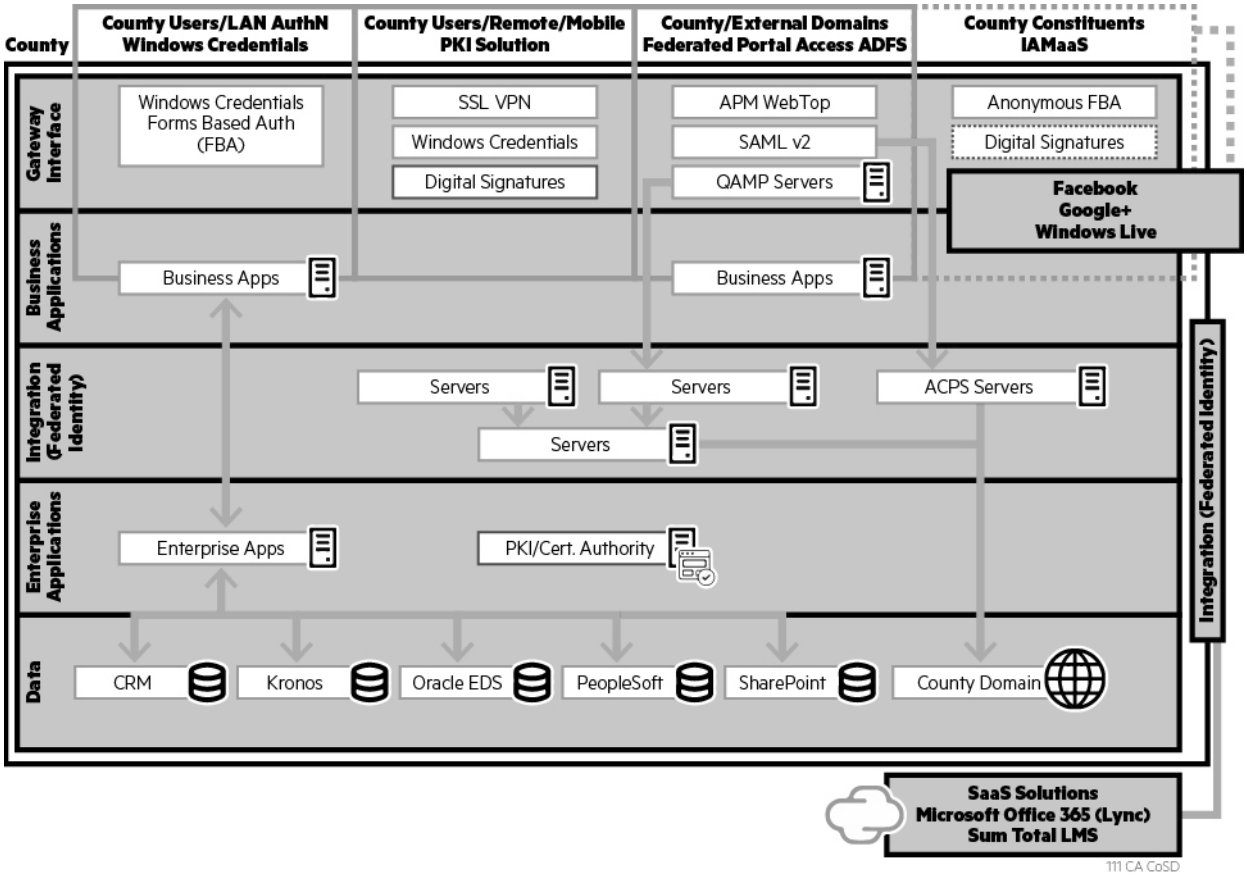
IAM Service	Hardware	Software	Support Labor
Active Directory (AD)	Infrastructure RU	N/A	IAM RU
Active Directory Federated Services (ADFS)	Infrastructure RU	N/A	IAM RU
Oracle Identity Access Management (IDAM)	Servers RU – Production Servers (County Responsibility)	Third Party Agreement (County Responsibility)	IAM RU
Public Key Infrastructure (PKI)	IAM RU (Luna Appliance Maintenance) Infrastructure RU (Servers)	IAM RU (certificate maintenance: 18,000 devices, 10 organizational, 16,400 user)	IAM RU
ID Provisioning	N/A	N/A	IAM RU

Solution: Contractor shall continue to evolve and improve the County's existing investments in PeopleSoft, Active Directory (AD), and Oracle Identity and Access Management Platform (IDAM) to provide an overall platform to protect and manage individual identities, their authentication, authorization and roles, and privileges. The starting point or foundational element of the solution shall be the Oracle IDAM platform, which is an industry-leading, end-to-end security solution—providing components that protect applications, data, documents, and cloud-based services through a combination of flexible authentication and single sign-on, identity federation, and risk-based authentication and authorization. The IDAM solution—starting with the Oracle platform and extending to the current County Active Directory, PeopleSoft, Public Key Infrastructure (PKI), and Active Directory Federation Services (ADFS), shall provide an integrated, modular architecture. This architecture shall provide the County with the flexibility to deploy a complete solution that enables the integration of current platforms, existing applications, and third-party security services into a single solution—offered at a single price point.

The high-level scope of this solution shall be to use Oracle Identity Manager as the basis to manage the End-User accounts across various applications and integrate identities within Active Directory, PeopleSoft, and third-party applications that contain County identities. The Oracle Identity Manager shall act as a single point of End-User management for the administrator to create users and authorize the End-User to access the relevant resources across the County, while allowing the other key platforms that contain identities to continue. The Oracle Access Manager solution shall secure the application access with respect to organization applications. The figure below shows the main elements of the County Identity Management solution, which shall make use of existing capabilities while expanding the solution to meet all of the requested functions for the County. Depicted in the figure below are the four main "kinds" of identities that the County must manage/administer. These identities are as follows: "classic" referring to County users that exist on the County network, County users that are remote or "off-premise," and County identities that require a federated relationship with external services such as County partners, residents or visitors.

By implementing the architecture illustrated in the figure below, each "kind" of County End-User shall be able to be managed in a low-risk, cost-effective, controlled, and secure manner so that management of the identities can be performed from a single point yet extend to each kind of End-User. Included in this solution shall be access to the County business applications, federation capabilities, enterprise applications, and County data sets.

- **San Diego County Functional Architecture**



Providing secure IT services through comprehensive IAM.

This approach leverages the County's investments in Oracle, PKI, Active Directory, and ADFS; lowers the technical and operational risk by expanding on existing platforms; and enables the County to continue to execute its Identity Management Road Map and Strategic Plan.

The following Oracle elements are currently implemented within the County's IDAM Platform 11g Suite – IDAM Platform integrating them with Active Directory, PeopleSoft, and Contractor IAMaaS. The table below details each of the main elements of the integrated solution and what specific function they provide.

- **Solution Integration Components**

PLATFORM	CURRENT BUSINESS USE CASE	FUTURE BUSINESS USE CASE
Oracle Identity Manager (OIM)	Integration with PeopleSoft	Onboarding for new employees Manage Health Care partners for Curam

PLATFORM	CURRENT BUSINESS USE CASE	FUTURE BUSINESS USE CASE
		Provisioning applications users (Curam, EDPP, EBS, OBI, and other applications) Manage privileged accounts in AD and UNIX
Oracle Access Manager (OAM)	Provides Single Sign On (SSO) to 25 applications to County employees as well as firewall department users Federation with firewall department organizations as Service Provider	Continue to integrate more County-owned applications. Federation with third-party vendors as Identity Provider. Future capability to provide SSO capability to third-party vendor applications like Adobe Cloud, Adobe Analytics, LexisNexis, ABC Legal, Accurint, Attorney's Brief, Empinfo, e-Oscar, Inverify, Past-Employ, The Work Number, Westlaw, and Pacer. Future capability to provide risk-based multi-factor authentication capability for IDAM protected applications. Future capability to provide SSO capability to State-owned applications like CSE (CCSAS), CA Central, CALWIN, ECSS (State IVR), KidStar, and SAT C3.
IDAM architecture	Provide High Availability within one data center	Future capability to provide IDAM architecture as a Zero Downtime Architecture (requires re-architecture of the environment.)
IDAM Infrastructure monitoring	Monitor software components manually	Leverage licensed Oracle monitoring tool, Oracle Enterprise Manager (OEM), to monitor IDAM infrastructure (both software stacks and data base).

Contractor shall provide the following Identity and Access Management (IAM) Services as a component of the Cross Functional Framework and included in the IAM RU:

- Active Directory Security: provisioning of privileged IDs, service accounts, group policy and organizational unit management, synchronization service for Skype for Business and role based access implementation
- Midrange Security: provisioning of UNIX, local Wintel IDs
- Active Directory Federated Services
- PKI: Symantec PKI services for device certificates for laptops and mobile devices. Other devices shall be covered and included at the completion of Transition, at no additional costs, as per the Transition.
- Oracle IDAM platform (11g Suite):
    - Identity Manager, Access Manager, Internet Directory, and Virtual Directory integration with Active Directory and PeopleSoft.
    - Oracle Identity Manager integration with PeopleSoft.
    - Oracle Access Manager: federation with "Firewall Department" End-Users as well as Single Sign On to 25 applications for County employees and 'Firewall Department' users.

  - Oracle Federation Manager: Service Provider capability which allows the "Firewall Department" Users to utilize their own AD ID and password to access County applications via an interface with ADFS.
  - Oracle IDAM architecture: support high availability infrastructure within the Tulsa Data Center, scalable centralized directory service, manual monitoring of software components.

- Participation in architecture and strategy sessions with the County to advance and maintain the IAM roadmap
- Maintain the Identity Access Management Services Management Plan
- Maintain the Service Desk for all End-User IAM related Service Requests. Actions performed by the Service Desk are covered by the Service Desk RU; actions performed by IAM personnel are covered by the IAM RU.
- Ensure maintenance of overall security of the IAM solution, including adhering to County policy in the provisioning of IAM services and compliance with any applicable regulatory process
- With the exception for the server and storage costs, which are not included in the IAM RU, for all IAM supporting infrastructure, Contractor shall provide labor for break/fix, maintenance, availability management, patching, and IDAM activities resulted from hardware refresh.
- For all IDAM supporting software, Contractor shall provide point releases (e.g. x.1, to x.2), upgrades, and system documentation as part of the IAM RU. Contractor may require a Service Request for any work efforts in excess of $500,000.

Contractor shall provide integration of the PeopleSoft and Oracle Identity Access Management (IDAM) as part of the project in progress as of the CED titled "Automated Interface to PeopleSoft Application for IDAM Services." Part 1 is funded in accordance with the applicable Work Request and it is currently scheduled for completion in June 2017. Ongoing support for Part 1 and Part 2 for the resulting integration is included in the IAM RU.

Exceptions

The following services and related support shall <u>not</u> be included as part of the IAM RU, Transition or Transformation services.
These are either dependent on the implementation of other requirements, requires an assessment of line of business application compatibility to utilize the functionality, or fulfilled in conjunction with other requirements. These shall be part of the IAM Roadmap and require funding to design, implement and support.

- Additional use cases or additional applications for Service Provider and Identity Provider capability
- Onboarding additional applications to use enterprise single sign on functionality
- Onboarding additional applications to be provisioned via automated workflow process
- Consolidation of disparate End User accounts into IAM Implementation and related support of roadmap activities
- New functionality or services identified as part of future roadmap activities not already scoped in Transition

- Resource and Facility Approach Summary – deployment plan for resources and use of facilities

The Contractor team supporting the County shall work closely with the County CIO, CTO, and supporting staff and provide a close-knit working environment that allows for direct communication, service, and for the County to be able to reach out directly to Contractor for quick resolution of any issues. Contractor's Rancho Bernardo facility is the center of support for staff specifically assigned to support the County, and is the initial point of contact for the County for service. Other subject matter experts within Contractor's Identity and Access Management practice and portfolio virtual teams shall also provide support and service as needed. The Contractor's Tulsa Data Center in Tulsa, Oklahoma shall host the majority of County IT infrastructure and core IT services. This shall include the infrastructure for ADFS, Oracle IDAM, and Active Directory. The Contractor Continuity Services center in Colorado Springs shall be the designated disaster recovery (DR) site.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Key Processes

By incorporating the HP Global Method (HPGM) for Identity and Access Management, Contractor shall take an iterative approach, addressing issues and improvements in data quality and data management—in practice and in implementation. Through this process, Contractor shall work closely with the County data teams and other transformation, integration, and architecture (TIA) data architects to define and manage County IT outsourcing enterprise data semantics. HPGM for Identity Management advocates a rapid, incremental, and iterative approach that can be aligned with the County's hybrid development methodology of "AgileFall."

In addition to HPGM Contractor shall also use a standard TOGAF-based architecture approach to develop the solution artifacts and produce the required documentation to make certain that the solution is not only documented correctly, but also minimizes the overall implementation risk to the County. These methods shall be integrated with the County's current Architecture and Solution Reviews in conjunction with the County's CIO office and relevant County departments.

For the Oracle IDAM Suite, Contractor shall work with the current Contractor IDAM architect to make certain that the design, development, and deployment of the Oracle IDAM Suite follows standard Oracle design and deployment methods to make sure that the Oracle platform operates within the design parameters. Any significant design changes to the platform or changes to the Oracle Databases shall follow Oracle-mandated practices.

The Computer Services Registration Form (CSRF) and process shall be replaced to meet the County's requirement to develop automated workflows to manage access Service Requests. Contractor shall leverage the Oracle Identity Manager product to automate the Access Service Request process. Automation shall include the ability to create a request with all appropriate validations, route it for approvals, email notifications, and predefined reports. The Oracle access request feature shall integrate with the Service Portal as well as the automated provisioning capabilities that are specified in Schedule 4.3 Operational Services.

Any remaining requirements not in place at CED shall be included in the IAM roadmap.

Describe End-User account consolidation plan and End User Account Management Architecture.

Contractor shall develop a plan for account consolidation and management architecture as follows:

- Use the County Strategic Plan to provide the architecture vision for IDAM.
  - The County Strategic Plan is to build enterprise-grade identity and access. Re-architecting IDAM to become a Zero Downtime Platform to serve the application community is a future capability.
- Use the Oracle Identity Manager to manage all End-User accounts (expand existing capability via the "Automated Interface to PeopleSoft Application for IDAM Services" project stated above).

  - Currently, the County relies on the Computer Services Registration Form (CSRF) process and manual administration to manage End-User accounts. Contractor shall build a capability into Oracle Identity Manager that creates network and email accounts automatically when a new employee joins the County. It deactivates the accounts when an employee leaves, based on data fed from the County Human Resource System. Contractor shall build capability into Oracle Identity Manager so Contractor can manage Service Provider accounts.
- Contractor shall utilize End-User data within PeopleSoft to manage the life cycle within the Oracle Identity Manager (via the "Automated Interface to PeopleSoft Application for IDAM Services" project stated above).
  - Use PeopleSoft to determine the life cycle of an ID.

    When a new employee joins the County, the Human Resources system shall be the authoritative source for identity data. For the County, this is its PeopleSoft (PSFT) application, which shall have a record for each employee. Oracle Identity Manager (OIM) shall be integrated with PSFT, and when a record is provided for a new employee, then OIM shall create accounts automatically in the County's Active Directory and Exchange environment. When an employee leaves the County, PSFT shall indicate such activity, and OIM shall inactivate the corresponding accounts in AD, Exchange, and other End-User stores. When an employee transfers to another department or business organization, then OIM shall receive notification from PSFT and take action based on established business rules. As the authoritative source of identity information, PeopleSoft shall be the driver of any necessary actions by OIM, and the process shall be automated with little need for manual administration.

  - Actions taken on the County End-User accounts shall be based on business rules established within the County such as hire, termination, transfers, leave of absence (LOA)/return from leave, and re-hire.

    As described above, PeopleSoft shall be the driver of the actions taken by OIM. Although the actions taken by OIM are triggered from PeopleSoft updates, the actions themselves shall be directed based on business rules that can be integrated into OIM. For example, if the trigger from PeopleSoft is a transfer between one department to another within the County organizations then rules can be programmed into OIM that would disable access to one type of data and allow access to other data if that was the policy. In the case of a termination notification from PeopleSoft, OIM would disable Active Directory and Exchange accounts.

2.19. Reporting Management Services

2.19.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor shall develop, generate, and submit deliverables. Contractor knows the current reporting criteria and shall continue the current level of reporting without interruption upon Transition completion. Contractor shall identify necessary reporting additions and enhancements to be completed as part of the overall cross-functional transition timeline. As part of the transition process for each framework, Contractor shall develop that framework's new report set (as identified in the RFP), either as a new report, or as an update to an existing report, where applicable. As the new reports are completed, Contractor shall begin posting them on the Service Portal. During the Cross-Functional transition, Contractor shall also implement Microsoft SQL Server Business Intelligence to begin the process of the data warehouse development. The data warehouse shall provide a central repository that supports other analytic scenarios as determined by reporting and County/Contractor quarterly review. Contractor is committed to continuous improvement and, over time, Contractor shall work with the County to extend both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured through increased system availability, reduced system disruptions, predictive analysis of system changes, and optimizing staffing levels.

Specific areas of ITSM that can benefit from analytics:

- Service Strategy and Improvement Analytics: This area shall focus on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis

- Service Design Analytics: This is a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data Contractor can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.

- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

Service Operations Analytics: Blending ITSM data and baseline IT performance data, Contractor shall conduct analyses to reduce business impact of events, incidents, and problems.

Post-transition, through a coordinated effort, Contractor shall identify specific subject matter experts for each reporting requirement and match them with a County counterpart to make certain that any new requirements are identified and supported for each of the Schedule 5 reports. In addition, Contractor shall demonstrate new and additional reports that the County finds valuable to manage their IT infrastructure, as well as streamline the reporting process as new transition and transformation tools are applied. The County shall have near-real-time reporting with fresh data to proactively monitor service performance and to take necessary actions. Service Manager provides 100+ out-of-box (OOB) reports; intuitive UI helps to create easily navigable role-based dashboards to show only what is applicable to a particular role. Each report shall have the option of printing and exporting (PDF, MS Excel, and HTML). Service Manager also has built-in reports for KPI reporting.

Rationale: Contractor shall have a well-documented and dynamic reporting management operation. Contractor's data analysts and Cross-Functional leadership shall be responsible for making certain that reports are generated accurately, on time, and in accordance with design or agreed-upon specifications.

- Resource and Facility Approach Summary –deployment plan for resources and use of facilities

The County shall continue to receive the current reports during the transition period. Contractor shall work with the County to consider new and improved reports through conducting workshops and meetings for the County to consider modifications to existing reports or to make new reports. These collaborative sessions shall be conducted by Contractor resources at its facility in Rancho Bernardo or at County sites identified by Contractor's customer.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall provide to the County all reports via the Service Portal. Contractor shall provide these reports and track the usage to provide feedback to the County on reports in high demand and those that potentially could be modified to provide additional value or possibly sunset.

Contractor shall create an analytics and reporting data warehouse during the transition period, based on MS SQL Server Business Intelligence, to facilitate ongoing automation and continuous improvement in efficiency and quality of Contractor's reporting capability.

- Use of Tools

Contractor shall use tools and data extract processes in the course of producing reports. The appropriate tools and products to be used in producing each report shall be finalized during the transition period, but shall consist of, at a minimum:

- Microsoft SQL Server Business Intelligence
- Microsoft SharePoint
- Contractor End User Access (Service Portal)
- EMC Documentum (DocVault)
- Various scripts and development tools, as appropriate

2.20. Domain Name Management Services

2.20.1. Process and Procedures

- Solution to meet the requirements and the rationale

Solution: The request for a new Domain Name (DN) and add-on DN services shall be initiated by the County point of contact (POC) via an IMAR request to the Contractor Service Desk or a project requirement. The Domain Name Administrator (DN Admin) treats either request as authorization to purchase the DN and DN services from an accredited registrar/vendor.

The Contractor Service Desk routes the IMAR request to the DN Admin, who takes the following actions:

- The DN Admin shall check the DN Portfolio for an existing account for the requesting department. If the requesting department has an account, then the DN Admin uses the existing account for purchase or creates a new account if one does not exist.
- The DN Admin shall save the confirmation receipt for future reference and adds DN and DN services to the DN Portfolio in the Integrated Asset Management System (IAMS).
- The DN Admin shall then email the County POC the confirmation of purchase and gives the County POC an initial username and password.
- If the requested DN is not available, the DN Admin shall email the requestor for an alternative DN.

The DN Admin shall be responsible for (1) actively monitoring the renewal of DN and associated DN services and (2) acquiring approval from the County POC for renewal. The DN Admin shall take the following steps for renewal:

- The DN Admin emails the County POC about DN renewal approximately 30 days before the expiration date. If there are DN services associated, then the DN Admin also requests DN services renewal.
- The County POC responds with approval to renew the DN. If there are DN services associated, the County POC also indicates whether or not to renew the DN services.
- The DN Admin pays renewal fees to the accredited registrar/vendor for the DN.
- The DN Admin updates the expiration date on the DN Portfolio accordingly and enters it into the IAMS.
- If the County POC decides not to renew the DN then the DN Admin updates the DN Portfolio in the IAMS.

The County POC may request cancellation of a DN and associated DN services prior to its expiration. The DN Admin shall treat these requests as authorization to release the DN and associated DN services. The following are the procedures for cancellation of a DN:

- The County POC submits an IMAR-Remove ticket in myRequests.
- The Service Desk routes the IMAR-Remove ticket to the DN Admin.
- The DN Admin cancels the DN and associated DN services with the registrar/vendor, removes the DN from the DN Portfolio, and saves the documentation in the IA.

The DN Admin minimizes the number of registrars/vendors from whom they purchase DNs for ease of management and transition of services. The DN Admin shall purchase/renew DNs for no more than a 1-year subscription to minimize the cost to the County in the event that a cancellation occurs. Contractor shall consolidate domain names to only accredited registrars, as each DN comes up for renewal.

The DN Admin shall create an Annual Domain Name Management Plan that details all DNs in the DN Portfolio, expiration dates of existing DNs, and any changes in DN management procedures. The DN Admin shall also create and post to the Service Portal a monthly report that shall include the following:

- Domain Name
- Total quantity of managed Domain Names
- Quantity of new Domain Names added in the last month
- Quantity of Domain Names retired in the last month
- Quantity of Domain Names retained by the County
- Summary data for each Domain Name:
  - Domain Name ID
  - Type/extension
  - Renewal date
  - High Org
  - Low Org
  - County POC name, email, and phone
  - Secondary County POC name, email, and phone.

Contractor shall provide Domain Name Management Services is for unlimited number of domain names.

- Deployment plan for resources and use of facilities

Domain Name management is performed by Contractor's Domain Name Administrator, who shall reside in Contractor's facility in Rancho Bernardo.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall conduct the Domain Name management in accordance with the agreed-upon Domain Change Management process with the County. Contractor shall implement continuous improvement in accordance with the Contractor's ISO 9000-certified processes and Contractor's adherence to ITIL processes for service delivery, including the review, analysis, prioritization, and recommended improvement opportunities.

The Domain Name Portfolio shall be stored and continually updated in the Integrated Asset Management System.

2.21. Business Analyst Services

2.21.1. Process and Procedures

- Description of solution to meet the requirements

Solution: Contractor shall establish a team of business analysts. These analysts shall create, gather, analyze, communicate, and validate requirements related to new IT projects or changes to existing applications, processes, or policies. The Contractor business analysts shall engage all County and Contractor stakeholders as well as contractor roles across the applications, engineering, testing, End-User support, and security towers. Contractor's solution recognizes the complexity of this role and provides tools for multifunctional teams.

Contractor shall work closely with the County business owners and users. Business analysts have an advanced level of knowledge and expertise within the particular industry or client they support. Contractor shall field a mix of experts who know the County's business well and are strong in eliciting and documenting requirements. This hybrid approach to staffing the Business Analysis Center (BAC) gives the County the optimal mix of knowledge of its business and functional/technical expertise from outside the County. The implementation of the BAC shall include:

- Flexibility in the business analyst staffing arrangement. - Analysts shall be available through a pool of resources the County can use on request or exclusively for specific projects or objectives.
- Shorter delivery time to meet customer demands. - As the County has direct contact with Contractor business analysts that can act as a bridge between requirements definition and solution development, it can improve and enhance service delivery to its employees and constituents.
- Experience in aligning the right resource to the right effort. –Contractor's solution for business analysis focuses on the identification, training, and development of experienced business analyst professionals.
- Quality and standardization in requirements identification and development. – As part of the BAC, each analyst benefits from a common set of industry standard best practices as defined by the BAC and approved by the County. These processes shall not only define behaviors and methodologies for assisting the county to develop the quality SOWs and requirements documents that are necessary to expedite project outcomes but also to create a smooth transition from identification of business needs through the project request process, requirements development, and beyond.
- Continued engagement throughout the project life cycle. - Business analysts shall participate in post-requirements phases, for example, guiding End-User acceptance testing and acting as training and documentation SMEs.

To support the solution, Contractor shall leverage its Enabling Delivery and Global Excellence (EDGE) methodology and toolset to develop the standard processes the team shall follow. EDGE is a repository of best multifunctional methods, tools, and processes that inform the creation of a custom, repeatable solution.

Rationale. Contractor's executive leaders are advocates of continued and expanded business analysis support.

Business analysis services shall meet the following objectives:

- Support the County by increasing the maturity, consistency, cost-effectiveness, and overall business value of business analysis services by developing a BAC
- Provide the right mix of County business knowledge, technology expertise, and business analysis expertise
- Provide a methodology and tools with flexibility for all types of projects, regardless of size or complexity
- Provide access to embedded business analysis resources via the BAC
- Provide portal-based access to a business analysis methodology tailored for the County
- Assist with business analysis training for County users via the BAC. This training shall be focused on project-specific needs
- Keep all processes lean and responsive to the County without creating too many procedures for business analysis to allow for expedited delivery
- Provide business analysts with the right aptitudes, certifications, and ongoing training.

- Deployment plan for resources and use of facilities

Contractor shall provide a pool of business analyst resources to be guided by common and flexible best practices and tools, which shall improve the quality standard for requirements gathering.

Contractor shall be flexible when assigning the work locations of all analysts to meet the needs of the projects and departments. Analysts shall be located in either the Contractor's Rancho Bernardo facility or an embedded location within the County. If a County department wants a dedicated resource, Contractor has that flexibility and shall work with the County to identify the best resource and solution.

Following Contractor's flexible, hybrid approach, Contractor shall provide an opportunity for current business analysts to gain more training and certifications as part of their professional development. Contractor shall develop talent and enhance staffing where necessary to meet the County's needs. In addition, Contractor requires specialized business analysis training, experience, and certifications when engaging new talent. Incoming business analysts shall demonstrate at minimum:

- Business- and technology-related education and experience
- Professional experience performing business analysis services
- Exceptional communications skills and strong interpersonal skills, including structured and unstructured facilitation
- Ability to understand and document functional business requirements and to translate business requirements into technical requirements and/or solutions
- Experience with formal business analysis methods and tools
- International Institute of Business Analysis (IIBA) Certified Business Analysis Professional™ (CBAP) certification or similar is a plus.

- Processes in solution including year-to-year continuous improvement

Contractor shall publish a County business analysis methodology on the Service Portal and use the BAC to help use and extend best practices throughout all County projects.

Enterprise-Level Best Practices

Contractor's first three best practices shall be implemented at the enterprise level. Through enterprise-wide standardization, a common language, and traceability, the County can create well-defined requirements that provide consistency throughout the application life cycle and become part of the County culture.

Enterprise-wide standardization - By standardizing requirements management at the enterprise level, the County can promote collaboration and eliminate silos between business analysts, development, and quality assurance (QA). A single system for complete requirements management provides the most up-to-date information for project teams. This is particularly important as requirements change over time, either because of changing business conditions or by design as part of an iterative development process such as Agile. A single requirements management system also enables better oversight.

Common language - Providing consistent guidelines for the language used for all requirements makes requirements easier to write and follow. This prevents both the overwork of adding more detail than necessary and the extra time needed to cycle back for more information when descriptions are too vague.

As a guideline these quality metrics include:

- **Lines of text**—the number of lines of text in the requirements document. When there is uniformity in the way requirements are described, this metric allows the End-User to estimate the functionality and degree of testing required for the software.
- **Imperatives**—the number of imperatives in different categories, such as "shall," "must," This number gives a rough estimate of the degree of design functionality required in the software. It also gives an estimate of the degree of testing required to satisfy these imperatives.
- **Weak phrases**—the number of weak phrases such as "large," "fast," "enough," etc. Weak phrases indicate vague design requirements that are non-testable.
- **Completeness**—the percentage of requirements that do not contain phrases such as "TBD" (to be determined) and "TBS" (to be specified). Requirements containing these phrases are considered incomplete.
- **Option phrases**—the number of phrases such as "can," "may," "I/we think," and so forth. These indicate requirements that might be difficult to satisfy in development.

Another best practice to encourage the use of a common language for requirements is to provide a template or set of templates for requirements definition.

Traceability - Contractor shall enable traceability throughout the application life cycle to determine whether a project meets requirements. The ability to bi-directionally trace links between requirements and testing.

Traceability metrics include:

- Requirements traced —number of requirements traced to or from each specification
- Requirements untraced—number of requirements that are not traced
- Requirements inconsistently traced—number of requirements inconsistently traced
- Linkages—number of upward and downward linkages for each requirement. This helps determine reuse and the impact of changes on the overall application
- Coverage—percentage of requirements traced to passed tests, failed tests, or tests not run.

Project-Level Best Practices

The next four best practices occur at the project level. Adopting these practices brings clarity to the requirements process and helps eliminate rework in application development and testing. In addition, these steps help eliminate overwork and rework in the requirements definition process itself.

Be lean. Do not create requirements assets unless they provide value to the application team. The assets with the most value are the ones that can be reused. A lean approach includes automating processes and eliminating waste. By systematically organizing requirements, it becomes easier to see which requirements are needed and which can be eliminated. Standardizing the content of requirements—with templates and a common language—helps make requirements easier to understand and eliminates rework.

Iterate. Create requirements iteratively to generate feedback, promote collaboration, and enable teams to identify defects early in the software development life cycle. A best practice is to start with a high-level business requirement by describing who needs the functionality for what purpose and why. Then, rather than working in isolation, the business analyst writing the requirement gathers feedback from major stakeholders on whether the high-level requirement adequately describes the business need. Developers also provide feedback on whether there is enough information to begin coding. If not, the business analyst drills down to add more detail. If there is enough information, the developers can get started.

Different requirements require different levels of detail. The County can save time and reduce complexity by providing just enough elaboration. There is no need to over-describe requirements that are easily understood.

Requirements assets that can be reused, such as business process models (BPMs) that can be used to generate requirements, provide the most value.

As a project goes through iterations of requirements definition, it is important to measure where and how requirements change over time. Change metrics include:

- **Volatility**— number of requirements added, deleted, and modified, classified by a reason for change.
- **Initial allocated requirements**—number of technical and nontechnical requirements originally provided by the customer. This metric, along with final allocated requirements and changes per requirement, describes how much requirements change.
- **Final allocated requirements**—number of technical and nontechnical requirements that were used to build the final software product.
- **Changes per requirement**—number of changes made to each requirement.
- **Changes over time**—number of changes per week, for example. This describes the degree of requirements volatility. This number decreases towards the end of the software life cycle, indicating convergence of requirements.

- **Cause of change**—categorizing the cause of changes helps in identifying the most common reasons for change and can be used to improve the software process.
- **Source of change**—identifying the source of change (that is, who requested the change) helps anticipate the sources for change in the future.

Visualize. Contractor can use visualization to increase understanding of requirements and the dependencies between requirements. Visualization makes it easier to identify potential problems, such as missing use cases. And pictures can be easier to read and navigate than text-based requirements. For teams that do not want to follow the Agile practice of writing code early in the process, visualization and simulations can be used to elicit early feedback to achieve many of the same objectives.

Collaborate. Collaborate and break down silos between groups from the beginning of the process. For instance, while a business analyst might have the End-User view of what a requirement should be, collaborating with the development team helps determine whether implementation of the requirement is feasible.

When these best practices are implemented, Contractor projects are more likely to meet intended business metrics, including budgets, schedules, and client satisfaction by eliminating the gaps between work processes performed in IT silos.

Standardization and Best Practices.

Embedded in Contractor's methodologies are common best practices that can be tailored to suit the County's needs, including those from BABOK, CMMI, ISO, and SSE. These methodologies integrate business analysis with the other development disciplines to verify continuity of standards through the project stages.

Gather and document County business functional requirements when working with County departments.

Contractor shall leverage its Enabling Delivery and Global Excellence (EDGE) methodology and toolset. EDGE is a flexible repository of best multi-functional methods, tools, and processes that Contractor shall tailor for each County project.

Contractor Business Analysis Services relies on a set a proven best practices, but is highly flexible for the County. Contractor shall draw on a pool of business analysts who have a mix of experience and diverse technical expertise and functional knowledge of the County and its businesses. The analysts shall work directly with the County user groups to accomplish the following:

- **Gain Broad Involvement**. Review documented high-level requirements with internal stakeholders, including representatives of those capabilities who shall be responsible for delivering the solution.
- **Define Goals and Requirements**. Confirm that defined detailed requirements support the business goals and provide compelling business value. Reconfirm boundaries for: business functions, current systems, internal and external interfaces. Confirm stakeholder and End-User profiles, business processes, End-User interfaces and use cases, interface requirements, business rules, data entities, non-functional requirements, geographic regions, language/culture considerations, volumetric(s) (e.g., how many reports were anticipated), and documentation.
- **Define Scope**. Identify perceived gaps in boundary definitions as issues. Document questions and assumptions with regards to understanding the high-level requirements. Transfer knowledge of detailed requirements and estimating assumptions (if any) from solution architect to business analysts and project team.
- **Use Leverage**. Leverage the experience of the detailed requirements development team and transfer knowledge to the solution delivery team. Review assumptions and constraints. Identify perceived barriers to evolving the detailed requirements into a solution. Confirm common understanding of the detailed requirements with client stakeholders. Review and discuss gaps, issues, questions, concerns, and assumptions.

- **Build Consensus**. Determine if the client and project manager agree that the detailed requirements are sufficient for solution development. If the detailed requirements are not sufficient, work with project leadership to assess the impact of delays resulting from rework of the high-level requirements. Raise requests for change as needed
- **Document Results**. The output of this work is a Business Functional Requirements Document. Once the functional requirements are agreed on, documented, and approved by the County, they can be translated into technical requirements or directly into a solution depending on the complexity and functional nature of the requirement. Contractor shall use templates that are already in use with the County and supplement them as needed with best practices templates from EDGE.

With this process and approach, the County users are involved every step of the way and own approval of the final Business Functional Requirements Document as the baseline for next steps in implementing a solution.

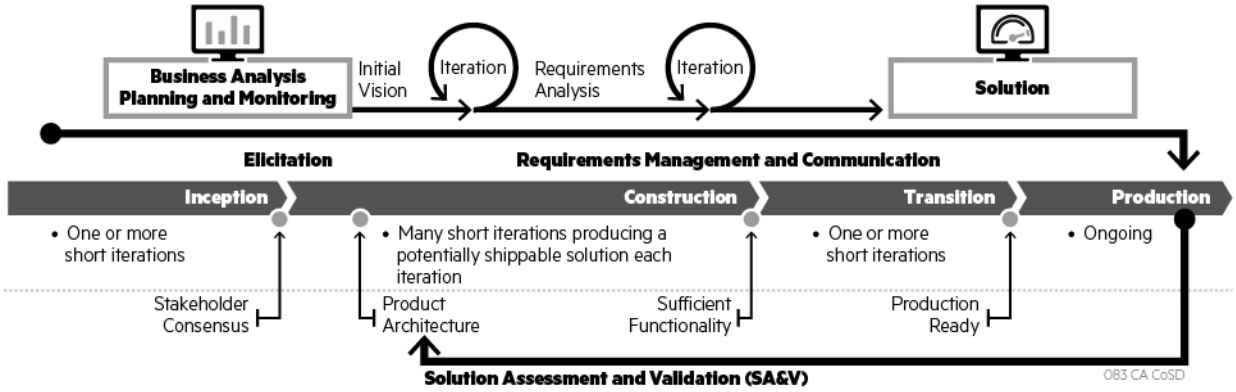
Translate business requirements into solutions or technical requirements.

Contractor's Business Functional Requirements Document shall include:

- Review Functional Business Requirements and confirm joint understanding of the requirements (this process is streamlined and low risk if HPE business analysts helped develop the functional requirements.
- Assess functional requirements and technical components required to meet requirements
- Map all functional requirements to technical requirements
- Ingest and consider technical alternatives and review with the County
- Make build versus buy decision and gain County approval
- Iterate technical specification and solution versus functional requirements to optimize business case – discuss tradeoffs with users and gain their approval
- Perform SIT and UAT
- Deploy

Contractor has a comprehensive process for this translation and solution development, as illustrated in the following figure:

Process to Translate from Requirements to Solution



Contractor shall provide a streamlined approach to reach a solution provides sufficient process control to achieve success.

Additionally, Contractor use the following best practices when translating requirements into solutions:

Once requirements are developed and refined, Contractor and the County may also conduct a Build versus Buy Analysis that identifies a "best-fit" solution based on requirements and budget. The best return for the County

comes when business requirements, staffing, and technology are optimally aligned with both End-User and mission needs. The business analyst's job is to analyze needs, document requirements, and identify optimal solutions.

Build. Contractor shall execute the requirements elicitation approach identified in planning until sufficient information is gathered to document the detailed requirements and estimate the cost to build. This cost can be compared to cost to buy COTS, and a final build versus buy decision is made. Contractor shall refer to previous iteration/release documentation as needed to shape the scope of the detailed requirements elicitation.

Depending on the nature of the build, Contractor shall decompose high-level information; abstract low-level information; distinguish requests versus needs; and distinguish requirements from design constraints. Identified requirements shall include functional/system requirements and may include non-functional requirements (such as performance, environmental, security, etc.), service-level requirements, quality requirements, and project management-related requirements deemed critical for project success.

Contractor shall store the collected information (such as informal or formal documents, meeting minutes, interview notes, emails, and other similar items) in a repository for future reference. Contractor shall document the decision criteria and justification for selecting the build option. Contractor shall select a build process, which leads to a build or development phase.

Buy. A COTS solution may be the lowest risk and least costly way to meet End-User functional requirements.

Contractor shall validate high-level requirements against the selected COTS product and perform a detailed assessment of the gaps to confirm that the essential requirements can be met (out-of-the-box, by configuration, or by customization). Business analysts shall be trained in the use of the selected product (including the features, flow, and architecture) or Contractor shall include COTS SMEs in the elicitation activities to clarify how the COTS product can meet the requirements or the impact of potential customizations.

Contractor shall store the collected information (such as informal or formal documents, meeting minutes, interview notes, emails, and other similar items) in a repository for future reference Contractor shall document the decision criteria and justification for selecting the buy option.

Ensure Business Analysts have the necessary level and type of expertise to perform functional responsibilities.

Contractor's approach to ensure that business analysts can perform successfully for the County has four elements:

- Recruiting and Hiring.
- Professional Development.
- Coaching and Feedback.
- Ongoing Experience and Professional Development

Through consistency in Contractor's processes and diversity in its projects, Contractor's business analysts gain growth and experience opportunities they cannot obtain elsewhere. This helps in retention and in the professional development of Contractor's business analysts.

2.22. Chief Technical Architect (CTA)

2.22.1. Process and Procedures

- Description of solution to meet the requirements

The Chief Technical Architect (CTA) shall be responsible and accountable to lead the development and delivery of strategic technology solutions that fit the business' needs. The CTA shall work directly with EAA and County Technology Office to review business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, align with information management strategies and overall efforts to continuously improve the provision of Services. The CTA shall manage and promote the use of County standards, related to software applications, promote the reusability of existing services and expanded use of County platforms, serve as a subject matter expert to projects and provide support for IT project teams.

Contractor shall use the methodology illustrated in the figure below, which is based on recognized and proven Open Group practices (HPES RightStep, IT Solution Architecture [ITSA] and The Open Group Architecture Framework [TOGAF]).

Contractor's EA Methodology

Contractor's approach enables change and transformation and provides the linkage between key stakeholder groups including business leaders, IT leaders and architects, and Contractor to achieve business transformation.

- Deployment plan for resources and use of facilities

The CTA and the Architects shall be two major components of Contractor's technology team. The CTA shall have overall responsibility for setting Architectural direction and strategy (with CTO), identifying emerging trends, anticipating and understanding transformative shifts in technology, developing enterprise and departmental roadmaps, and maintaining strong relationships with Contractor's leading technology partners. The CTA shall then translate this information and direction to the Architects for execution.

The Architects, who shall receive strategy and direction from the CTA, shall be responsible for executing that strategy including adherence to methodologies, standard processes, best practices, accelerators, and standards.

The CTA shall report to the Account Executive, and the Architects shall report to the Contractor's Technology Office. The structure unencumbers the CTA from the administrative burden required when one has direct reports, including HR activities and staff professional development—these activities shall be the responsibility of the Contractor's Technology Office.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall adhere to proven methodologies and processes across the organization that it adapts to meet the County's requirements.

Contractor shall align with its proven architectural methods (RightStep and ITSA) and holistic focus that encompasses business, data, applications, infrastructure, network, security, management and implementation aspects including solution evolution.

Solution Design Documents

SECTION TITLE	CONTENTS
Executive Summary	<Write a brief introduction describing the focus of this design document including, if applicable, the purpose, background and scope that affect the design of the project. This summary should be written in nontechnical terms as an introduction to the technical sections. It should contain enough information for a reader to get familiarized with what is discussed in the full document.>
Client Opportunity	[Use this section to describe client opportunities, problems, business drivers and/or goals. Include quotes or comments from clients if appropriate. Where appropriate, personalize the document for the client, mentioning the customer name and specific topics related to their environment.]
Proposed Design	<This section describes the logical and physical solution design including the physical architecture. Include one or more diagrams of the design either as an embedded picture or in the appendix. It is important to highlight that this template just provides guidance which must be tailored by the architect or engineer for their specific work. Not all sections and subsections are applicable to all solutions, and there may be some key ones missing for the solution you are designing. This is a template to help jumpstart the work at hand and provide ideas for design content that otherwise might be left out.>
Business Architecture	The business architecture defines the manner in which business strategy/mission, vision, governance, organization and key business processes come together to define the activities that deliver on the business strategy. Business architecture can be developed with a scope that encompasses an enterprise or solution scale. <This section is used if the impact to business from the implementation of this solution needs to be understood by the client stakeholders. For example, if there are significant changes to the way the client does business {business processes, roles of the client employees, business organization, etc.) here you would describe the logical changes to the business architecture. Each section would include the current and proposed architecture.
Data Architecture	< Data architecture provides a blueprint for the structure of the information components in the context of the business processes and the business organization, the application systems and their interactions (integrations), as well as the relationships between them. This includes the data, data service interfaces, and data management components and can be developed with a scope that encompasses an enterprise, solution or technology scale.
Applications Architecture	< Application architecture is the blueprint for the individual application systems to be deployed, their interactions (integration) and their relationships to core business processes of the organization. Application architecture can be developed with a scope that network requirements or touch points.
Infrastructure Architecture	Infrastructure architecture describes the software and hardware that effectively enables the deployment of other architectures. This includes IT infrastructure like servers, storage, backup devices, End-User devices, middleware, processing and standards used in operations, and does not include the network or communication components which have their own section. Infrastructure architecture can be developed with a scope that encompasses an enterprise, solution or technology scale.
Network Architecture	Network architecture describes the software and hardware that effectively enables the connection between infrastructure components and architectures. This includes networks,

SECTION TITLE	CONTENTS
	firewalls, load balancers, WAN, LAN, VLAN, communication devices and appliances, infrastructure device placement within the network, and the associated network standards used in operations. Network architecture can be developed with a scope that encompasses an enterprise, solution, or technology scale.
Security Architecture	< Security architecture is the blueprint for the structure of the security components of the overall solution, and how they are maintained in line with the security policies, both principles and requirements. It provides the central definition of the capability independent threat and vulnerability structure as well as disaster recovery. A security architecture can be developed with a scope that encompasses an enterprise, solution or technology scale.
Acceptance Criteria	<Describe the success criteria and acceptance requirements guidance. This is at high level; acceptance test plans are created later in the lifecycle guided by these criteria but with much greater detail. This is to provide guidance to the architecture and design on how successful outcome is measured by the stakeholders/client. business acceptance criteria would be those measured in terms of business goals, drivers, metrics, outcomes or results, if any ("Improve claim handling productivity by XX%">. Functional acceptance criteria by those that measure what is included (if the many areas of scope were included, functionality of given modules or components, non-functional requirements or qualities). Technical acceptance criteria are related to "how" the solution is put together (how the layers are put together {three tier architecture for example}, how the interfaces work, how the roles are spread across the many environments, etc.). Implementation acceptance criteria revolve around "with what" and in what order the solution is made {for example, database was required to be on Oracle, middleware and ESB using TIBCO, small project implemented first and later phased to full production, support personnel training, documentation standards and content, etc.}.
Implementation Considerations	<Describe the items that were addressed during the design phase of the project for implementation.>
Deployment	<Describe the technical details of the solution's deployment. Include architecture diagrams.>
Infrastructure Management	<Describe how the infrastructure is to be managed, operated and which companies or organizations are responsible.>
Maintenance Plan	<Provide an explanation of the ongoing maintenance support model. Include reference to any existing agreements as well as any new procedures, processes or resource units.>
Evolution	<Describe the evolution requirements or special considerations that affect project planning and solution implementation aspects—order of implementation of the many components, changes in solution scale /size during the various implementation phases, bringing in highly specialized or hard to find resources, etc. This is not a repeat of other sections of the solutions, this is an extract of what project managers should watch for and take into account in the implementation, testing and development planning.>

RightStep and ITSA shall align with the Contractor framework and governance for consulting services, to facilitate integration with all other supporting methods and disciplines—grouped under the umbrella of the Contractor transformation framework. This framework shall align and integrate the architecture with other Contractor capabilities and methods that are necessary for successful transformation including business consulting, value management, management of change, program and project management, portfolio management, IT service management, SOA services, and governance.

Use of Tools

To create architectural designs, Contractor shall use modeling tools such as EA Sparx, ProVision, and/or MEGA to represent business processes, models, and patterns that define the business architecture. To address IT transformation challenges, the Contractor architecture team shall introduce MEGA as the business intelligence tool to provide comprehensive visibility across business functions, application components, servers, networks, system software, and financials using imports from PPM and County AppsManager. Using EA life cycle processes (for example, BRICK) and principles, MEGA enables comprehensive enterprise portfolio management to identify core systems, systems of differentiation, and systems of innovation to facilitate alignment with County business strategies.

Application Architecture

Contractor's applications architecture shall include application principles, integration models, application landscape models, application portfolio maps, application to process maps, application flow models, application to information matrix, and application standards, among others. These are organized within topic areas (sometimes called domains and subdomains) and supported by RightStep, as described above.

Staffing and organization of Architecture Services.

Contractor's global architecture capability is an organization with a formal charter and governance model within ES that supports all aspects of architecture services—methodologies, processes, best practices, accelerators, standards, and professional development. This applies to all architects, whether enterprise, solution, business, or technology architects. This is consistent with Contractor's approach to create architectures that seamlessly provide guidance from the enterprise scope to the solution and technological layers. The guidance and standards provided by the ES architecture capability team is also used by other business units. Architecture capabilities/teams reside throughout Contractor's organization, in both accounts and in local and regionally available teams that can be leveraged as an element of a client engagement. To facilitate the organization of architecture services, a collective set of standards, best practices, tools, and accelerators for each strategic capability are kept within the Contractor's EDGE platform.

Common architecture toolset and documentation standards

Contractor architects shall regularly conduct whiteboard sessions with other team members— security, application, the County, and other vendors—before Contractor creates an SDD for any project. The updated SDD template, included in the Solution Summary and Rationale section above, shall cover all necessary architecture artifacts and design consideration, which shall include high availability, scalability, County architecture/network patterns, reuse of existing County technology assets, leading to complete, consistent and coherent solutions. Contractor shall also use this document for internal reviews as the standard template for architecture projects from start to finish. Every SDD document shall also be used in its entirety in downstream activities, for example, by engineers for technical design documents, run books, server builds, load balance workbooks, and firewall changes. This approach facilitates consistency across all projects from design through implementation.

2.23. Enterprise Application Architect (EAA)

2.23.1. Process and Procedures

- Solution Summary & Rationale – Description of solution to meet the requirements

The Enterprise Application Architect (EAA) shall be responsible and accountable for the "advise to manage" (illustrated in the figure below) portion of the enterprise architecture, while supporting the CTA, CISO and County Technology Office in the "strategy to technology" portion. The EAA shall work directly with CTA and County Technology Office to review business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, align with information management strategies and overall efforts to continuously improve the provision of Services. The EAA shall manage and promote the use of County standards, related to software applications, promote the reusability of existing services and expanded use of County platforms, serve as a subject matter expert to projects and provide support for IT project teams. The EAA shall provide the bridge between County business and the IT staff that ensures that the application architecture meets business goals and objectives, that promotes reusability and provides data and interface connectivity across the Enterprise.

CONTRACTOR'S EA Methodology

- Resource and Facility Approach Summary –deployment plan for resources and use of facilities

The CTA and the EAA are two major components of the Contractor's architecture team. The EAA shall serve as a technology lead and liaison to County business in developing and linking technical solutions that meet requirements and act as a subject matter expert on the effective use of technology in developing County business solutions. Working with the CTA, County Technology Office and CISO, once overall architectural strategy and direction has been established, the EAA shall advise IT staff regarding the feasibility of their proposed approaches to project solutions in terms of systems capabilities, new technologies and alignment with established application architecture guidelines and standards. The EAA shall have overall responsibility for IT strategy execution across the enterprise including adherence to methodologies, standard processes, reference IT patterns, accelerators, and standards.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall adhere to proven methodologies and processes (RightStep and ITSA) across the organization that are adapted to meet the County's requirements. Contractor's Architecture Services Methodology is based on principles that the County Technology Office has adopted—principles precede requirements and they help frame the overall solution approach to align with County strategic direction.

Processes: Contractor has two primary architecture methods recognized by The Open Group (HPES RightStep and ITSA). Since the EAA is focused on solution development across the lifecycle, the EAA shall primarily use Contractor's Global Method of IT Strategy and Architecture (ITSA). ITSA is Contractor's methodology for

developing solution, initiative, or technology architectures. It is a structured as a participatory approach that involves key stakeholders in the client's business. It has been proven effective through many years' experience in defining, guiding, and evolving complex information systems in multiple application domains. ITSA helps architects understand the needs of all stakeholders by viewing the architecture from four vantage points or views:

- Business View – *Why* is the engagement being done? What are the motivations and business drivers?
- Functional View – *What* will the system do? What information will it provide?
- Technical View – *How* will the system be realized with IT components?
- Implementation View – *With what* specific products and other components will the system be implemented? In what organization? According to what plan?

ITSA defines each view using principles, models, and standards appropriate for the business domain. When combined, the four views enable Contractor to understand the needs of all stakeholders and create a snapshot of the solution. Business factors (drivers, goals, metrics, principles, models, and standards) are the basis for all technical and implementation decisions. The methodology does not specify (or limit) the techniques to use to gather the business information or products to solve the customer's problems and compliments each client situation to determine business need, maturity, and existing standards.

- Automated Tools

To create architectural designs, Contractor shall use modeling tools such as EA Sparx, ProVision, and/or MEGA to represent business processes, models, and patterns that define the business architecture. To address IT transformation challenges, the Contractor architecture team shall introduce MEGA as the business intelligence tool to provide comprehensive visibility across business functions, application components, servers, networks, system software, and financials using imports from PPM and County AppsManager. Using EA life cycle processes (for example, BRICK) and principles, MEGA enables comprehensive enterprise portfolio management to identify core systems, systems of differentiation, and systems of innovation to facilitate alignment with County business strategies.

2.24. Innovation Management Services

2.24.1. Process and Procedures

Innovation Management Services shall support the transformation and innovation model of continuous progressive change in how Services are delivered. This shall include, but is not limited to, delivering Services via a bimodal approach, with an emphasis on exploration, agility, and speed, while still maintaining operational integrity and stability.

Innovation Management Services shall begin at Transition completion with presentation of a qualified Innovation Officer (IO) to the County for County approval. The IO shall develop for County approval a program charter and rules of engagement that define the process to:

- identify potential needs/issues/gaps/opportunities for improvement
- create a list of potential services available to further innovation and transformation, to include:
    - joint development workshops
    - white-board sessions
    - prototypes
    - pilots

  - demonstrations of products, software or services
- design and develop lab environment(s) and rules of use
- determine method to define success criteria
- define collaborative engagement model with EA, CTA, EAA, CISOs and County Business Leaders

Innovation Management Services shall include an Innovation Management Office that shall serve as the foundation for continuous business improvement, innovation, and transformation. The Innovation Office (IO), planned for January of CY2, shall be composed of the Innovation Officer and additional on-demand resources, upon County Approval with the directive to drive IT innovation/transformation and create a true environment of agility and high-velocity change at the County.

The IO shall create and update in the Standards and Procedures Manual the necessary information for the Innovation Management Review Board.IO shall work with County Technology Office and County Business leaders to identify specific actions in support of County Excellence Goals. This results in a series of initiatives in which Contractor shall propose solutions, business case analyses, anticipated pricing, and project timelines and resource plans. The proposed initiatives shall be reviewed by the Innovation Management Review Board and, if approved, shall be executed using (as appropriate) agile and rapid-prototyping methodologies.

- Resource and Facility Approach Summary –deployment plan for resources and use of facilities

The Innovation Management Office shall be a virtual office with some members residing at CAC and Contractor's Rancho Bernardo facility and others at US-based facilities as determined by skillset required.

Starting after CY1, Contractor shall provide Resource Units rates for the following three (3) resources or more to be used on-demand, upon County approval:

- Senior Technologist (skillset akin to CTA)
- Senior Solution Architect
- Senior Business Analyst

The above resources shall be billed at the Innovation Core Team Member rate as defined in Schedule 16.1 (Fees) – Exhibit 16.1-1 or any applicable labor category rate if it is lower. Any of these labor category rates are to be consumed against the 50%/50% jointly funded Innovation Fund as defined in Schedule 16.8 Fee Adjustments.

Additional personnel ebbs and flows through the Team as required by Innovation/Transformation ideas/pursuits/opportunities.

Additional personnel may come from the County, Contractor, Contractor's partners or other 3rd parties and could include:

- Business Leaders
- Senior Technologists
- Innovation Lab Personnel
- Local Government advisory personnel (e.g.: Gartner)
- Architects/Engineers
- Business Analysts

- Software Specialists
- Logistics Engineers
- Mobility Specialists
- Change agents
- Logistics experts
- Asset and Billing Specialists
- Government Strategists

At execution, Contractor shall propose utilization of an existing RU aligned with the skillset of the team member. If an existing RU cannot be utilized for the activity to be performed, Contractor shall propose an hourly rate or FFP for County consideration. Rates shall be agreed upon in writing by the Parties.

- Processes including year-to-year continuous improvement

Methodologies and key processes shall be defined by the charter and rules of engagement.

Governance shall be provided by the Innovation Management Review Board, co-chaired by County CIO and Contractor AE who shall have joint approval on all proposed initiatives and activities.

Contractor shall perform an annual assessment of Innovation Management Services for County review and approval as part of Schedule 5 reporting requirements.

3. SERVICE DESK SERVICES

3.1.1. Process and Procedures

The Contractor solution to meet the requirements

The following shall be the various support tiers and transfer types used by Contractor:

Support Tiers:

Tier 0 – Self Service
Tier 1 – FCR (anything that can be addressed by the initial agent with no transfer)
Tier 2 –Ticket transferred to a second level agent for support for resolution of an issue requiring on-site support or additional administrative permissions (typically applies to feature functionality issues i.e. Operating System, Browser, MS Office Programs, etc.)
Tier 3 – Ticket transferred to a 3rd level agent (framework) for resolution. Datacenter, Applications, Security, Network, Vendors/3rd party, on-site, engineering, etc. Feature functionality issues typically require specialized support and advanced permissions to resolve the issue
Tier 4 – Global administrator/engineering/architecture required to resolve the issue

Unless otherwise provided in the script documentation the following Transfer Types shall apply:

Transfer Type	Description	Priority
Cold	Ticket sent straight to frame work in the ticketing system with no communication	P4/P5
Warm	Chat E-mail Text	P3/P4/P5
Hot	Phone call	P1/P2/P3

The Contractor Service Desk for the County shall serve as a single point of contact and the primary owner for monitoring and tracking of all incidents and Service Requests (SRs) for approved End-Users. Contractor's key solution strategy is to use ITIL-aligned processes to meet requirements, achieve 70% first-call resolution (FCR), and achieve 12-minute phone handle time as well as Service Desk ownership for end-to-end tracking of all tickets and SRs. Contractor's Service Desk shall use a knowledge documented in the electronic Knowledge Management System (EKMS) to make a swift determination on whether an issue is warm transferred to Contractor's remote desktop/device management (RDM) capability or escalated to deskside/field support or the appropriate framework (e.g., Applications M&O, End User, Network).

Contractor's updated training processes shall provide agents with in-depth knowledge of County processes, scripts practice, and ITIL-based practices. Contractor shall ensure all employees including new hires receive Contractor's Doing Business with the County instruction and monitor individuals for its completion. Contractor integrates the training activities Contractor's agents receive with real day-to-day work assignments. Contractor's training increases agent comprehension of County-specific issues and expertise in routing tickets efficiently and effectively to the appropriate technical support group. shall identify those agents who require additional instruction and customize training to strengthen their skills.

As Contractor implements the self-service technologies of the Agreement, Contractor shall encourage users to access the Service Portal's self-service functionality from their desktops, tablets, or mobile phones. Contractor shall provide its technology End-User adoption approach,

Contractor's HPSM system's data analytics functionality shall include documentation and display on the Service Portal of Service Desk statistics tied to both Contractor's team's objectives and the County's service levels. The data warehouse, accessible through the Service Portal, shall contain County attributes for reporting and analytics such as PA-ID, POETA, County Group, and County Department. Contractor's Service Desk manager shall perform quality reviews on relevant areas such as call waiting/call abandonment, efficiency in meeting the phone time to resolve metric, rate of FCR success, and End-User satisfaction levels upon ticket resolution. On systematic review of trends, surveys, and reports, the Service Desk manager, together with other members of the Contractor account management team, shall find opportunities for improvement of Service Desk services and operational cost efficiencies.

Service Desk Structure

Service Desk.

Contractor agents shall be the first point of contact and if needed shall provide remote desktop/device management (RDM). If support requests cannot be resolved by the first contact agent (Level 1), then the call shall be escalated to RDM (Level 2). In some cases, the Service Desk agent escalates to the deskside/field team or subject matter technical support (Level 3), which includes frameworks such as applications, engineering, exchange, data center, infrastructure, storage, etc. Level 1 and Level 2 resources shall reside within the Service Desk Framework. Level 3 support shall be provided primarily by the various frameworks unless the Service Desk has the ability to resolve the issue based on the documentation provided by the framework and has the required access to the systems. Contractor shall provide to all agents Service Desk training and detailed documentation outlining the correct escalation path for each type of incident or SR that guides agents to make certain that tickets requiring escalation are routed correctly the first time.

While the Service Desk Framework is responsible for the full life cycle and management of all incidents, installs, moves, additions, and removals (IMARs), and SRs, each framework shall be responsible for management of its work stream, making certain that work is triaged within the required timeframes. Points of contact (POCs) are identified within each group to manage these activities and verify work is completed. Costs associated with these activities outside of the Service Desk agents shall not result in additional costs to the County.

Remote Desktop Management (RDM). Service Desk agents shall use RDM to interact with network services, software systems engineering, and/or an applications group to restore service and/or identify and correct problems. This may require assisting in simulation and recreation of End-User problems and recommending systems modifications to reduce End-User problems. Service Desk agents shall be facilitators between customers and other support teams to make certain customer needs are met and tickets are resolved in an expeditious manner.

Comprehensive Service Desk for the County

Contractor shall continually add to the knowledgebase, working closely with other resolver groups to identify areas where Contractor can improve knowledge documentation to provide increased resolution at first call, freeing resources to support their other activities.

Deployment plan for resources and use of facilities

Resource Management — Oversight for Service Improvement. The Service Desk manager shall provide oversight of performance, resource management, and service delivery, including the collection, consolidation, and dispatch of events and information sent by the County as it relates to the environment. As part of this role, the

Service Desk manager shall review metrics on customer satisfaction and success in meeting County requirements and establish quality processes and intensified training approaches to improve Service Desk performance. Contractor's reporting analyst shall analyze Service Desk data, identifying and adjusting metrics queries, and fulfilling the ad hoc Service Desk-related report requests from the County and from the Contractor service delivery manager in the County.

The Service Desk manager shall lead daily status calls with the Service Desk Workflow Manager (Workflow Manager), operations manager, and shift leads to make announcements, communicate County concerns, and review the status of any issues that emerged overnight. In addition to the daily status calls, the Service Desk manager shall call meetings every Monday before each shift begins that include the agents on deck. These meetings shall provide a venue for management and agents alike to raise issues they need to address and to foster interaction with the Service Desk manager in his efforts to support alignment with County expectations. Contractor's Service Desk support shall concentrate agent numbers in shifts during the County's core hours from 6:00 a.m. to 6:00 p.m. PT, Monday through Friday, and maintains support overnight and weekends.

The Workflow Manager shall support the Service Desk manager in providing day-to-day supervision of operations, monitoring that agents arrive on time and are attentive to their responsibilities, adjudicating rotation of shift personnel, and making sure that the metrics gathered on Service Desk are uploaded properly on the Service Portal for review by the Service Desk manager, the quality analyst, the Contractor account team, and County administrators. The workflow manager shall constantly communicate with the Service Desk manager, updating him on Service Desk issues throughout the day, workloads, and staffing, including issues of individual agent performance.

Working with the Service Desk operations manager and scheduler, the shift leads shall monitor the ticket queue to make sure tickets do not go unattended. Other shift lead responsibilities include providing oversight of ticket agents' handling of Priority 1 and 2 Incidents and High Response End-User/Critical User tickets. Contractor's shift leads shall oversee agent performance and work with the Service Desk's training analyst to develop measures to improve expeditious handling of tickets and effective agent–End-User interaction. Contractor's training analyst shall check the training history of individual staff, making certain that all staff take Contractor's mandatory training, and shall provide follow-up as necessary.

Key methodologies and processes including year-to-year continuous improvement

IT Service Management (ITSM) Processes for Service Desk. Contractor shall implement ITIL/ITSM processes for Service Desk with a focus on customer service satisfaction and continuous improvement. As a key ITSM framework process, Contractor's Service Desk shall own and track tickets created at initial call or that are assigned via the Service Portal, and it is their responsibility to maintain open communication channels with the End-User in the event of a ticket inquiry throughout the ticket's life cycle. Contractor's Service Desk agents shall also provide an interface for activities such as SRs, customer change requests, incident management, and third-party support.

Continuous Improvement. ITSM shall collect data from the Service Desk system, Customer interactions, HPSM, the Avaya CMS Call Manager, and the Customer feedback surveys that Contractor uploads for data aggregation and review. All of the data input from these systems along with the additional reporting that Contractor adds from chat and Self Service shall be placed into the analytics environment that is created in support of the Service Portal. Service Desk related data shall be posted to the Service Portal and reviewed regularly with the CTO during the Operations status calls.

Quality Monitoring to Improve Agent Overall Performance and Customer Service. Contractor's Service Desk manager together with the workplace manager and shift leads shall review the results of the customer satisfaction surveys and other relevant data displayed on the portal (for example, phone handle times at initial call, ticketing information, chat data, most common scripts used, etc.) to discover areas for improvement, discuss them with the

quality assurance (QA) analyst for Service Desk, and present findings at a Monday all-hands Service Desk meetings for each shift.

At these meetings, managers and leads shall make recommendations on issues identified or for the agents to raise new problem areas they have experienced the previous week. The workplace manager shall upload results and new resolutions from the meeting to the Service Desk dashboard reserved for agent posts. As each shift conducts its Monday meeting, additional comments shall be added to the dashboard. These recommendations shall be communicated by the Service Desk Manager to the CTO.

Contractor shall implement the following five-step quality management framework, supported and documented by Contractor's QA analyst: (1) Monitor Performance; (2) Analyze Performance; (3) Identify Areas for Improvement; (4) Establish Corrective Actions; and (5) Verify Improvement. The framework aligns with Contractor's seven-step ITIL processes for continuous service improvement.

Monitoring Performance of Individual Agents. Contractor shall capture agents' voice interactions with users along with the corresponding computer desktop activities, such as data entry for logging tickets, cataloging and prioritization, screen navigation, and data retrieval from the knowledgebase. To effectively coach employees, Contractor shall use two quality monitoring methods: side-by-side and remote. In side-by-side monitoring, the shift lead shall use a headset to join the call of a new agent or an agent learning better communication skills. The shift lead shall also use remote monitoring—that is, agents are unaware they are being monitored—to audit and evaluate agents' performance for Contractor's quality metrics.

Contractor's Service Desk manager shall consult with the workplace manager and shift lead to perform agent evaluation review and identify patterns to assist agents in understanding how each aspect of their performance affects the whole.

Automated systems and tools involved in Contractor solution

Contractor shall implement for the County HPE Service Manager (HPSM), Contractor's system that includes comprehensive core and extended Service Desk advanced functionality. It shall provide key Service Desk automated processes and manage Contractor's responses to County users, including first call resolution (FCR), deskside support coordination, and ticket and SR escalation to support, including to AT&T network/mobile SMEs and other vendor support.

Contractor shall implement the Service Portal and its self-service capabilities within 90 days of the Contract Effective Date. The portal implementation approach as detailed in the Transition section for the Service Desk shall include the core functionality of new services and links to current data sources and source systems to integrate with current repositories within the 90-day timeframe.

At the end of the transition period End-Users shall be able to perform the following via self-service:

- online -ticket creation
- Review status of tickets and Service Requests,
- Perform online password resets via the Self Service Password Reset, SSPR tool
- Conduct chat sessions with the Service Desk for information or support
- View reporting.
- Access to the Knowledgebase (FAQs, tips sheets

- View Outage Status, Trending Now, and Announcements
- Access to MyRequests, and various links (ITSC, DocVault, etc.).

The new service catalog that replaces myRequests and the complete integration of the configuration management systems (Asset Manager, Apps Manager, ESL) shall be implemented as a part of the transition and is included under the Cross functional transition section and timeframes. Contractor shall engage the CTO and other relevant County stakeholders to provide input into the look and feel of the portal. County users shall be able to access the Service Portal, including self-service functionality, from their desktops and other platforms.

On-Going Maintenance, Support, and Enhancements: The Service Desk Manager shall be the primary point of contact for the Service Portal for the County of San Diego. Technical support and enhancements shall come from the Contractor's Portal framework, which is a leveraged team. The Service Desk Manager shall make certain that issues related to the portal are being resolved and that maintenance items and new features are being implemented as needed.

Contractor shall follow a quarterly maintenance schedule for changes to the portal that are non-incident related and for changes that may require coordination, training, and communication to the End-Users. Simple changes (adding links, contacts, FAQs, Announcements, Trending Now information, etc.) shall take place on a frequency agreed with the County. The overall focus around the processes and frequency related to these changes shall be to ensure the latest and most accurate information is published to the portal in a timely fashion to benefit the End-Users. Once the timelines are established, processes shall be built, approved and communicated as required. To make certain that the changes being made are communicated, well thought out, and in the best interest of the End-Users, the Service Desk Manager shall be a part of a Portal Review Board, the final composition of which shall be established by the CIO, in consultation with Contractor Account Executive, to discuss, approve, document, and communicate all changes related to the Service Portal. These changes shall include not only the content within the Service Portal but the processes related modifications that need to be made over time to ensure information and Service Portal accuracy. For changes to the Service Portal that require Portfolio Application modifications or County data manipulation, a Budgetary Estimate (BE) shall be provided to the County to determine how or whether to proceed with these changes.

Training: Training shall be provided for all End-Users and support staff as a part of the Transition project related to the Service Portal. This shall cover every aspect of what is in place at the end of this project. As a part of transition planning, Contractor shall discuss with the County the various training options and communications that are needed to ensure that all End-Users understand the capabilities of the portal and how the portal works.

Sample Landing Page for Service Portal with Self-Service Functionality

Unless otherwise agreed to by the County, the landing page for the Service Portal shall be substantially similar to the following:

County users shall be able to click a tile to phone Service Desk, open a ticket on their own, reset their own passwords, make SRs, check County announcements, access training, FAQs, and Tips, and stay alert to outages. In another example, upon clicking "Open Ticket," a dropdown menu appears that allows the End-User to select from a list of problem categories; once the category is selected, a second dropdown menu appears with category-relevant problem descriptions. During the process, if the End-User decides guidance is needed from a live agent, he or she can click the "Chat" tile or "Call Service Desk" for support.

When a ticket is created from the portal or the Service Desk via a phone call or email, Service Desk shall embed the End-User's profile (i.e., contact information, location, and asset information) in the ticket and track it until resolution, posting updates on the ticket's progress on the portal. The solution shall allow the End-User to easily obtain ticket status by accessing the portal landing page from his or her desktop, tablet, or mobile phone.

The fully-implemented HPSM shall include myRequests.

Ownership and end-to-end tracking of Incidents

Service Desk shall have ownership of all tickets and shall track them from End-User submission through ticket resolution. Contractor shall use ITIL-aligned processes. The Service Desk agent shall update the End-User on ticket progress until it is resolved.

Service Desk Handle Time and Escalation of Incident Tickets. When an End-User calls in an Incident by phone, the Service Desk agent who answers the call shall own the ticket. The agent shall first verify whether the call is for an Incident rather than a SR. Once an Incident is validated, the agent shall log the ticket, including the End-User profile, categorize the Incident, and prioritize the ticket according to the County's priority matrix (i.e., Priority 1–3); if the caller is on the High Response End-User list, the End-User profile shall automatically alert the agent to register the ticket as Priority 1 or 2 depending on the severity of the issue.

If the Incident arrives through an End-User-created ticket via the Service Portal, its automated processes shall upload it to the ticket queue for selection by available ticket agents. Ticket assignment order shall be determined by first in/first out and by severity. Severity 1 and Severity 2 tickets shall receive immediate attention by Service Desk agents, with oversight by the Workflow Manager and Shift Lead.

Once the Incident is logged, the Service Desk agent shall assign the ticket, start troubleshooting, and diagnose it using information provided by the caller or the description on the portal-generated ticket. The Service Desk agent shall quickly resolve low-level Incidents associated with known errors by applying approved solutions or workarounds. In cases where the Service Desk agent may know immediately that the Incident cannot be resolved, the Service Desk agent shall determine, based on knowledge documented in the EKMS, whether it can be routed to deskside/field support or to the appropriate framework for resolution. In some cases, vendor-specific support may be required. The knowledge incorporated in the EKMS shall derive from information provided by the vendor on its hardware/software; resolution and workaround instructions developed by Contractor's SMEs based on their respective areas of expertise (e.g., applications, network); and information developed by the County SMEs on its infrastructure.

Deskside Support Escalation. When Contractor's deskside technicians receive a ticket, they shall retrieve all the service attributes from the EKMS and launch scripts and perform progressive troubleshooting based on the documented knowledge to identify the probable source of a service Incident. For example, if Service Desk performs troubleshooting and is unable to resolve the ticket, the Service Desk agent shall itemize the actions taken and issues still unresolved on the ticket's Comments section. Service Desk shall notify the End-User that the ticket needs further troubleshooting deskside; the technician shall coordinate the date and time for the visit with the End-User and post the appointment in the ticket. The ticket information, including scheduled deskside visit, shall be viewable via the Service Portal.

Subject Matter Expert (SME) Escalation. When the Service Desk agent recognizes that the source of the Incident requires SME support, he/she shall escalate the ticket to the SME support team appropriate to the affected framework.

In addition, Service Desk shall escalate unresolved "child" tickets that match a "parent" ticket to the SME support team working on that Incident's resolution. The SME support teams shall perform additional diagnostics, as necessary, to identify and implement an appropriate solution or workaround. These teams shall take a comprehensive approach to resolution, keeping in mind the parent/child ticket linkage and recording their actions in the Comments section of the ticket accordingly. Once the issue is resolved, the Service Desk shall update the status of all the linked tickets on the Service Portal and notify all impacted users.

Vendor Support Escalation. When a ticket is escalated to a Third Party regarding a product that cannot be resolved by Contractor's deskside technicians, the Service Desk ticket owner shall confirm that the problem is fully described on the ticket before it goes to the vendor's helpdesk.

Ticket Closure. Once the ticket is resolved, the resource responsible for the resolution shall change the status of the ticket to "Resolved." This action shall automatically notify the End-User via email of the resolution. The body of the email shall request a reply within 3 days if the issue was not resolved to the End-User's satisfaction. If no answer is received after 3 days, the ticket status shall remain "Resolved" for an additional 7 days in case the End-

User is out of the office. If the End-User does not reply after the additional 7 days, the ticket shall automatically be set to "Closed." Contractor shall continue using this format to update the End-User on resolution if desired by the County, but at the County's option, Contractor shall implement a verification email that shows the End-User how the ticket was resolved, encourages the End-User to complete the customer feedback survey, and promotes the County's self-service password reset requirement. When the End-User clicks on the respective blue icons in this message, he/she goes to the Service Desk site related to the text.

Maintenance and refresh of Service Desk scripts.

Contractor shall use structured formats for receiving calls and scripts that have proven successful in addressing problems and accelerating resolutions within 12 minutes on Service Desk. Contractor shall develop scripts for RDM and higher-level technical solutions. When the County users request a new script or a modification of a current script, the appropriate technical support group shall communicate with them in developing the script in adherence with Service Desk Script Revision Process documented in the Standards and Procedures Manual.

Contractor's knowledge content analyst for Service Desk shall review scripts for consistency with the database methodology and style guide, recognizing that certain Service Desk scripts are spoken to the caller. Contractor shall maintain successful scripts in a Service Desk EKMS with rules-based access to Contractor's agents/technicians. Contractor shall refresh the information in EKMS and the Self-Service Knowledgebase information annually.

Contractor's Service Desk Manager shall adhere to the Framework Revision Process flow established by the County and post in the Service Portal Contractor's Monthly Revised Scripts—Revision/Acceptance Report, which enumerates the total scripts in the EKMS and the number of revisions that month.

Using HPSM, Contractor shall collect metrics on response and resolution times associated with respective scripts that Contractor's agents use against identified problems.

In reviewing metrics and issues raised by Contractor's agents, the Service Desk Manager shall identify less helpful scripts and assign them for rework. Contractor's development of new scripts or revisions of existing ones shall draw from the HP Global Service Desk scripts, a database of proven scripts to address a range of problems that have demonstrated success on Contractor's accounts worldwide.

Contractor's Service Desk shall support the Service Portal by reviewing the scripts in the EKMS and selecting those appropriate for revision for "how to" instructions with visual aids for upload into the Self-Service Knowledgebase. Contractor shall work with relevant SMEs in developing suitable language for End-Users accessing the Service Portal's self-help functionality. This shall include tips, training and FAQs.

Preventing abandoned calls

Contractor shall increase Contractor's training of Service Desk agents, both new hires and incumbents, to increase their ability to resolve tickets quickly. This training shall include Contractor's indexed Knowledgebase and scripts to resolve less complex Incidents quickly at first call. For callers making SRs, the trained Service Desk agent shall point the caller to the related content in the Service Catalog for products and direct the caller on how to use the SR tool on the Service Portal.

Additional Measures: Contractor shall take measures that shorten the phone handle time to restore service to the End-User as quickly as possible and allow the agent to help the next End-User.

- Contractor shall provide Contractor's agents with a Self-Service Knowledgebase with an indexed search engine at their fingertips;
- Contractor's agents shall open their response to the caller with a time-saving structured format (template)

- The call waiting recording shall provide the option for the End-User to leave voicemail to be returned within 15 minutes

First call resolution strategy

Upon receiving a call, the Service Desk agent shall access the Service Desk module's dropdown menu, which shall provide a range of predefined problems or SRs.

A Service Desk agent shall quickly assess the issue and determine if it can be resolved by the agent or must be escalated for SME support.

- Contractor shall identify data in HPSM to determine overall FCR performance, by contact type and agent identification.
- Contractor shall calculate the number of repeat calls on the same issue to identify trends and problems and develop Knowledgebase and "how to" articles accordingly, including tips and FAQs.
- Contractor shall identify Service Desk agents needing additional training.

Resolution of Impacts to County and non-County End-Users

The Service Desk shall quickly identify High Response End-User and critical systems issues, and shall page Contractor's appropriate on-site technical support.

Contractor's HPE Service Desk agents shall provide elevated support when it comes to critical events in the County. Critical or special events include but are not limited to the following classifications:

- County-wide disasters/emergencies. For these events (e.g., fires, floods, power outages), the Office of Emergency Services (OES) is activated and support personnel are required to work with the County to support the End-Users and the public. The size of these events vary, and Local Assistance Centers (LACs) may be required
- Disasters/emergencies that are small in scope. Response to these events (e.g., focused areas of flooding, building damage) are typically initiated by the Business Group that is impacted. In some cases, a relocation is required to continue to provide service, or an LAC must be stood up.
- Elevated service levels are activated for the Registrar of Voters in support of elections.
- Elevated service levels are activated for Treasurer Tax Collector in support of several public-facing activities conducted by the County.

Each of these events shall have a documented process in place to ensure that Contractor's agents and staff not only understand these requirements but also can route calls appropriately for resolution. The Service Desk agents shall have everything they need and be trained to support this effort and are able to distinguish between an emergency event and standard call.

Contractor shall update the High Response End-User priority matrix and a list of County and non-County High Response End-Users as provided by the CTO.

Calls, emails, or Service Portal notifications from these High Response End-Users and organizations shall be automatically flagged at the Service Desk for escalated response. The Service Desk agent receiving the notification shall follow the mission-critical workflow and the Workflow Manager shall provide oversight to make sure the call is escalated if it cannot be resolved right away.

On-site support to End-Users

The Service Desk agent may determine that deskside support is the necessary next step to resolve the ticket. Before escalation, the Service Desk agent shall review the ticket to make sure that all actions taken in diagnosing and troubleshooting have been recorded in the Comments section.

The Service Desk agent shall notify the End-User that the ticket requires a deskside visit for additional troubleshooting. Then the deskside technician shall coordinate, via Chat or on the mobile phone or email, the visit date and time with the End-User. The scheduled time, date, and location shall be updated in the ticket, which shall be available for lookup on the Service Portal.

Once the deskside technician resolves the issue, the ticket shall be set to "Resolved" and shall follow the "Ticket Closure" process described above.

Contractor shall locate Contractor's deskside support personnel at the Rancho Bernardo facility and at the CAC and COC. Contractor shall station Contractor's mobile phone personnel at the AT&T facility on Trade Street.

End-User self-service capabilities

Contractor's self-service solution shall provide End-Users the option of accessing the Service Desk to open a ticket, obtain ticket status, make an SR, check outages, and perform password reset via the Service Portal from multiple platforms, such as mobile phone, desktop, tablet, or Chat.

Chat. As part of the Service Desk transformation, Contractor shall enable users to use Chat with Service Desk agents to request information, report an incident, or request information on SRs. As with other methods of contacting the Service Desk, Chat shall begin with the standardized ticket workflow and ends with successful resolution. Agents can handle multiple, simultaneous text Chats. The chat tool shall come as a part of the HPSM toolset that is being implemented for the County. The End-User shall be able to access this chat functionality through the Service Portal so no additional software is required on the End-User's devices. **Self Service for Incidents/Problems**. The new self-service ticket capability option shall enable an End-User to open a non-critical ticket that is automatically submitted to the Service Desk queue for review and action. The End-User clicks on "Open Ticket" to submit hardware, software, connectivity, printing, phone, and voice issues, as well as general questions. Users shall be able to track their ticket status without contacting an agent by clicking the "Ticket Status" tile on the portal.

Self Service for Password Reset. As a part of self-service, Contractor shall implement HPE's Self-Service Password Reset Tool (SSPR tool). The SSPR tool delivers multiple ways for End-Users to reset their own passwords. This solution removes the requirement for Service Desk intervention where End-Users have forgotten their passwords and/or locked their account. SSPR is a web browser-based, automated password reset tool that uses dedicated infrastructure, within the County's domain. It also provides a Web-Services based API that allows password resets directly from the Logon Screen. SSPR can also be accessed by visiting the SSPR Web Page from any supported browser on any device, provided it is connected to the County's network. Integration with Active Directory shall be completed as a part of Transition. Other repositories to be added as requested by the County via Service Request.

Additional Self-Service Features. Contractor's portal capabilities shall include more features for both self-service and agent assistance:

- Knowledgebase search engine capability that provides users on their desktop, laptop, or phone "how to" instructions for resolving common problems. Contractor's Knowledgebase content shall use standard text information that delivers clear "show me" instructions that walk the End-User through resolution, click-by-click. It shall also provide videos for step-by-step problem resolution.

- FAQs based on Contractor's review of questions typically asked by users and Tips that enable quick search on a range of information.
- Self-service password reset online tool that allows users to securely reset their own passwords without agent intervention. Users access the secure system by a simple web-based interface, such as a County public-facing website, linked to the portal but implemented separately.
- Dashboard view of the end-to-end County IT environment. Both County management and users are also able to view Rich Site Summary (RSS) feeds, system-wide notifications, alerts, and other important information that impacts the overall IT environment.
- Mobile device "click to call" brings easy dialing options to contact a service

Contractor's approach to introducing the new technologies promotes early County administration and End-User adoption because self-service saves time and improves End-User productivity. Among Contractor's techniques, Contractor shall host training sessions for County users to demonstrate portal and self-service capabilities. On deskside visits, Contractor's technicians shall demonstrate functionality and answer questions. Contractor shall distribute tent cards with "how to" instructions on County desks.

End-User survey process

Contractor shall provide a customer survey for break/fix tickets. The format of the survey shall be designed to make it easy for End-Users to assess in as little as a few seconds the level of their satisfaction with the Service Desk and provide comments if desired. Contractor shall consult with the County on the final design of this survey; upon agreement, Contractor shall distribute the survey after ticket resolution via email or mobile phone. The customer survey shall be an automated process. The automated dispatch and collection of the survey shall be independent of Service Desk.

Contractor shall provide survey results on the Service Portal each month for the appropriate CTO staff. The survey shall identify the ticket agent and the type of issue that was resolved. HPSM metrics shall provide the time taken to resolve the issue and the tier level of resolution, including whether Contractor is meeting Contractor's 70% first call resolution rate.

Contractor's Service Desk Manager shall collect and regularly review the survey data collected; a reporting analyst shall identify trends and mentoring and training opportunities.

Continuous measurement of Service Desk performance

The Service Desk ticket system, phone reports, and customer interactions and surveys shall provide the data needed to the Service Portal. These data points shall provide the detail that not only makes certain that Contractor is meeting Contractor's service levels, but provides the level of information that Contractor requires to continuously improve Contractor's services.

The HPSM Service Desk module shall enable Contractor to standardize the collection of data, collect more categories of data, and provide more accurate data on which Contractor can identify areas that need or demonstrate improvement. For example, dropdown menus with predefined service issues shall allow Contractor to enumerate a standardized selection of issues and determine their average time to resolution. It shall also indicate agents who take longer than the average who may need more training, are working an issue that may require more documentation, or have come across something new that Contractor needs to put in place. Contractor shall follow ITSM processes in tying data collection and metrics to continuous service improvement.

The Service Desk Manager shall define the metrics needed to improve Service Desk customer satisfaction and shall use the HPSM Service Desk's data collection capability. HPSM logic shall be aligned with ITSM processes, thus allowing Contractor to collect data not only directly tied to the service levels but also more detailed data that support Contractor's strategy for continuous improvement.

Inputs to this step shall include collecting data against the service levels. HPSM shall have the capability to collect data automatically, including:

- Baseline data on call waiting times
- Call abandonment rates
- Initial call handle time
- Resolution time in Service Desk by agent
  - Categorization of predefined issues and their resolution time
- Customer Satisfaction Survey ratings and End-User comments

Service Desk Manager and Workflow Manager shall conduct a daily operations status call to review and report metrics and discuss issues that may have emerged overnight or are trending. This call shall take place before County standard business hours to ensure Contractor can resolve issues that were raised from the night before. Together they shall review data collected on Contractor's response and resolution times. They shall develop corrective action plans and implementation schedules to improve areas that are lacking or areas where new items need to be put in place.

HPSM has more than 150 reports that Contractor can use to gather information. The reporting and data that Contractor uses from this system can be filtered in any way necessary to for Contractor to either provide the information to those requesting it or to isolate the area in which Contractor need to improve or is making an improvement. Information from the various reports that are needed to support the business shall be provided to the County via the Service Portal and the various meetings that take place (CTO Operations Meeting, Portfolio Review Meetings, etc.). Contractor shall seek direction from the County on the reports to be displayed and who needs to view which set of reports as Contractor moves through Transition and build out of the Service Portal.

Contractor's ITSM-aligned, seven-step process, depicted below, provides a solid foundation for capture and reporting of data to support analysis that Contractor can use to identify opportunities for continuous improvement.

Seven-Step Process for Measuring Performance to Support Continuous Improvement

Error! Reference source not found. describes relevant Continuous Service Improvement (CSI) activities, such as service level reporting and management processes, that Contractor has tied to the Seven-Step Process:

Continuous Service Improvement Service Desk Approach for the County.

CSI ACTIVITIES	CONTRACTOR CSI APPROACH TO SERVICE DESK
Steps 1, 2, 3, 4 Performance Metrics	Contractor shall capture a performance metrics and capture the same metrics every month thereafter for comparison. Contractor shall display Contractor's metrics on the Service Portal metrics dashboard in a meaningful, easy-to-use format for access by Contractor's agents and the County. These metrics shall come from HPSM and the Avaya Call Manager system.

CSI ACTIVITIES	CONTRACTOR CSI APPROACH TO SERVICE DESK
Step 3 Customer Satisfaction Surveys and Assessment	In combination with the performance metrics that Contractor shall use in steps 1 to 4, Contractor shall leverage HPSM Service Desk to collect customer feedback using customer satisfaction surveys. Contractor shall regularly review customer satisfaction surveys and follow up on any negative surveys. This allows a feedback loop into the process for improvement as well as follow-up communication to the customer.
Step 5 Identifying Opportunities for Improvement	Contractor's Service Desk Manager, working with Contractor's Work Shift Manager and agent leads, shall use a real-time portal view of Contractor's Service Desk performance metrics (e.g., call waiting time, call abandonment, Service Desk time to resolution, volume of tickets escalated to different resolver groups), data analysis, and lessons learned to identify improvement opportunities for Contractor's Service Desk team of agents.
Step 6 Daily Agent Meetings Dedicated to Service Improvement	The Service Desk Manager, Work Shift Manager, and Service Desk agents shall meet daily to review areas that need improvement and brainstorm ways to improve performance. For example, if metrics show that Service Desk phone handle time has increased with the use of the script for break/fix, Contractor shall work together to see what phraseology is causing the problem and correct it.
Step 7 Corrective Action Development and Implementation	For serious quality issues, Contractor shall develop a Corrective Action Plan (CAP) with support from the accounts QA personnel that includes a timeline for implementation. Following implementation, Contractor shall gather metrics specific to the issue to measure progress.

Design for the Service Portal

Contractor shall use HPE Service Manager (HPSM) software at the core of Contractor's ITSM Service Desk. HPSM shall include Contractor's integrated Service Portal solution for providing a closed-loop incident process and End-User self-service Incident resolution, SR creation, and information search. HPSM together with the Service Portal shall provide multiple dashboards easily accessible by County users and Contractor management, and Service Desk agents.

Key components of the Service Portal Contractor shall include:

- Access from both the Internet and the County Intranet
- Support for key processes, including incident, problem, change, SR (interaction), self-service, and service asset and configuration management
- Single sign on (SSO) integration and predefined roles and rules
- Improved, standardized screen layout with "smart indicators" to flag related information
- Rich cross-process functionality via a range of wizards
- Management reports, service-level reports, all required County deliverables
- Service Desk-specific components include:
  - Service levels built in with data analytic capability that generates reports such as ticket volume and response times
  - Self-service access to the Service Desk to open a ticket, access the Service Catalog, make an SR (through the SR management tool), access ticket and SR status, see announcements including number of outages
  - FAQs, tips, training, and self-service password reset capability

- County-dedicated EKMS for technical support teams that includes documentation and flowcharts for processes, procedures, root cause analyses (RCAs), and high-level work around instructions across the frameworks

3.5. Service Request Management Services

3.5.1. Process and Procedures

A self-service indexed Knowledgebase developed specifically for access by all End-Users, upon County approval, to help them obtain the best answers in real time to their request for information and resolve low-complexity problems.

Contractor shall provide Service Desk agent assistance for fulfilling Service Requests (SRs) and to enable users to create their own SRs on the electronic processes of the Service Portal's self-service capability. Contractor's Service Portal shall use HPSM and myRequests, the current application for SRs and ticketing. The Service Portal shall also provide the entry point for other tools such as SharePoint. As part of the Cross Functional Transition phase, Contractor shall migrate myRequests to HPSM's more advanced SR functionality.

Contractor shall work with County to capture and document all SR-related content and maintain it in a rules-based database within the SR Management tool. Contractor shall also develop a Service Portal version of the OIC Service Catalog.

Service Desk Agent SR Assistance. Contractor's Service Desk agents shall assist users with submitting SRs for items such as installs, moves, additions, and removals (IMAR) or changes to the workplace environment.

Service Desk shall provide this service by creating records on SR forms, copying an existing record, or applying a predefined template that prefills specific fields using electronic processes:

- The End-User makes the SR to the Service Desk by phone, email, fax, or the Service Portal.
- The Service Desk agent determines if the SR is a request or an Incident and follows a closed loop process
  - If the request is an Incident, it is handled as discussed in the Incident Management Section.
  - If the request is an IMAR, the agent shall refer to the appropriate documentation to make certain that the request is routed properly to the appropriate framework. Details of this process are provided in the End User Services Section.
- The Service Desk agent categorizes the request and assigns a priority level.
- The Service Desk checks the Service Catalog, which is based on the OIC Service Catalog, to determine if the SR needs approval and, if so, the level of approval required.
- If a request is approved, the Service Desk agent escalates it as appropriate, and updates the End-User upon request.

Service Portal Service Catalog. Contractor shall develop a version of the OIC Service Catalog suitable for Service Portal self-service. The portal's version of the Service Catalog shall be accessible to all End-Users for making Service Catalog-based SRs. The SRs shall display the approval process required to the End-User before being routed to the Service Desk. A Service Portal version of the Service Catalog shall provide the following benefits:

- Reduces Service Desk's workload by providing self-service capabilities for Service Catalog requests that flag approvals that are required
- Ensures all self-service SRs are routed to Service Desk for review

- Provides a single, guided, questionnaire-style End-User interface for requesting support for catalog and non-catalog items
- Provides tablet and mobile End-User support.

4. END-USER SERVICES

4.1.1. Process and Procedures

Assessing and mitigating impacts to existing desktop systems and business applications while transitioning to new standard platforms.

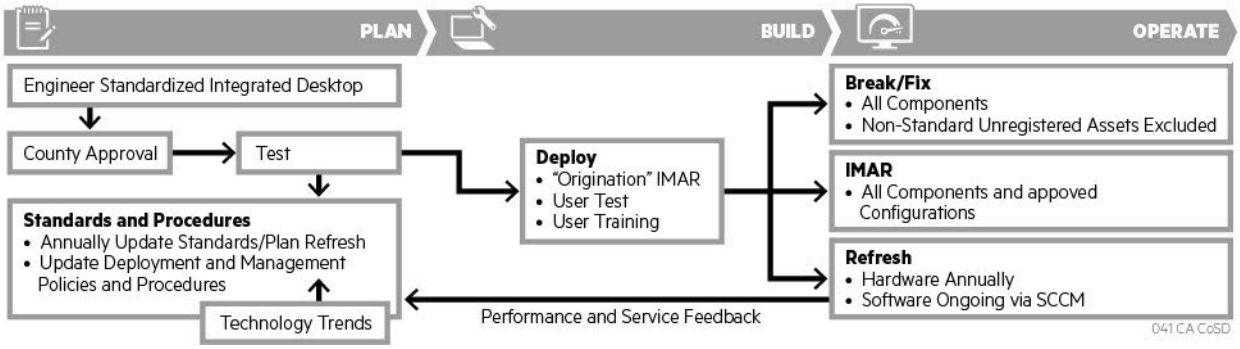
Generally, updates to the existing desktop environment, including hardware, core software, and OS, and all other components shall be organized as follows:

- **Standard Yearly Updates.** These are annual updates to the standard configurations for hardware and Core Software – the total "platform." Concurrently with these updates, hardware equipment that is due for tech refresh shall be scheduled so that all changes are made as one event.
- **Ongoing Updates and Refresh.** This activity entails ongoing, incremental, regular updates to approved configurations. Ongoing updates relate primarily to software. Contractor shall check the hardware inventory annually to determine which machines are eligible for refresh.
- **Ad hoc and Emergency Pushes** – Emergency pushes shall be event driven. Typically, these are defensive security pushes in response to vendor patches to protect the security posture of the standard desktop configuration and/or minor functional updates from the software OEM (versus major version upgrades, which shall be assessed more thoroughly and shall be part of the standard yearly update).

The figure below shows the Plan, Build, and Operate life cycle.

Enterprise Architecture and Desktop Engineering shall collaborate on changes to the standards—Desktop Engineering shall build and tests those changes and provide updates to the knowledge base and End User Service technicians via documented procedures and cross-training sessions.

End-User Services Framework



Standardization and Governance

The cycle for standards governance and standard desktop configuration updates shall be annually.

Standards shall be updated based on a County request, Contractor's assessment of the technology market, vendor presentations to the County, or other County initiatives. All requests shall be reviewed and consolidated. Contractor's engineering group shall lead the consolidation and analysis of these requests and bring the County a consolidated list of recommendations, which shall be presented to the Governance Review Board for approval. Once Contractor has received the County's approval, Contractor shall perform more detailed engineering and testing of the new configurations.

Process to Review and Approve Annual Updates to Standards. Major updates to the standard configurations and core software shall be made yearly, with a monthly rhythm. The timeline for annual updates to the standard configuration is shown in the table below.

Monthly Flow of Annual Standards

TIMEFRAME (MONTH TO MONTH)	ACTIVITY
Ongoing (January through December)	County performance trend analysis Industry trend monitoring User needs analysis
September through October	Current industry product assessments by Contractor team Vendor briefings to the County and Contractor
October	Draft updates to standards Review and approve new standards Update timelines/roadmaps
November through December	Perform desktop/core software testing and Systems Integration Test (SIT) Perform applications User Acceptance Test (UAT)
January through December	Deploy all tech refresh – annual updates based on device type and End-User-specific configurations Deploy software refreshes via SCCM

- Governance: Sponsored by the County CIO
- County participants include CIO and staff, and End-User representatives of each functional organization.
- Contractor participants include the COO, Account Chief Technologist, Technology Office Lead, Desktop Services Management, Applications Lead, and appropriate members from those organizations.
- Boards and Review Committees exist for Standards and Catalog management—such as the Configuration Governance Board (CGB) and Catalog Review Board (CRB).

Between the annual cycles and standards governance events, the Contractor's Technology Office shall host weekly Enterprise Architecture meetings with the County that review new technology trends, vendor roadmaps, and as needed, performance issues in the County environment. These meetings shall provide ongoing input once a configuration is fielded regarding immediate and/or systemic issues and provide a safety net to the annual engineering and testing cycle.

Engineering

Desktop Engineering shall be involved before and after standards are set up front with Enterprise Architecture to ingest new requirements, review new and emerging technologies, assess integration compatibility with current and fresh configurations, and recommend new standards. As new standardized configurations are rolled out, Desktop Engineering shall resolve Tier 3 tickets and systemic issues. The functions of Desktop Engineering, Integration Engineering, Enterprise Architecture, Applications Management and Operations, as well as Applications Development, IT security, and County business application owners shall work together to standardize and test desktop configurations and applications.

Major changes in hardware, operating systems, or other significant architecture upgrades shall receive more extensive engineering and testing.

Systems Integration and User Acceptance Testing. The Desktop Engineering group shall perform SIT and UAT testing using the test lab at the Rancho Bernardo facility. This test lab has multiple device types and

configurations to test against to confirm that configurations are ready for deployment. The Desktop Engineer shall conduct SIT with the Test Engineer when images are updated and created to make sure the image and software work properly. Test results shall be peer reviewed and any issues shall be resolved before production deployment. For major upgrades Contractor shall perform full regression testing – End-User, performance, and security – as part of SIT and UAT.

UAT shall be performed by both Contractor and County users on both types of applications. It shall be performed when an application is first requested and approved, and when there is a major upgrade to the core software and OS standards.

Overall, this methodology results in a new gold image for new deployments and an upgrade path/procedures for current desktops that may or may not require re-imaging the desktop depending on the scale and scope of the upgrade.

This methodology shall be governed by County procedures.

Specific Support to Business Applications.

Contractor shall have an End-User representative for each application. Contractor shall also have an entire Applications organization that shall be responsible for applications and their support.

There shall be two types of applications:

- Catalog Applications – Catalog applications shall typically be COTS; they shall be limited to 440. Contractor shall monitor the number of applications to control County expenses. Contractor shall continuously work with the County to help optimize the applications list. Catalog applications do not have backend infrastructure associated with them – they are software packages, typically off-the-shelf. They shall be installed on the desktop and have no interaction with any other components (i.e., no database or servers it needs to talk to).
- Portfolio Applications - Portfolio applications shall be supported by the Contractor applications team and shall typically be hosted in the data center, on a two-tier or three-tier architecture (thus servers and databases are involved, along with a desktop client most of the time). With Portfolio applications, the project team (more than just desktop engineering, to include the DBA and application SMEs) shall be involved in SIT before it goes to UAT.

Some portfolio applications (e.g., Kronos) require unique configurations or n-1, n-2 desktop configurations that are not the current standard. Contractor shall accommodate these needs on a case by case basis. Contractor shall work with the County to improve the standardization of these exceptions.

Desktop Computing refresh activities as well as maintenance and upgrades to the Desktop Computing Core Software, including the Operating System.

Contractor shall update the existing desktop environment as follows:

- **Standard Yearly Updates.** Annual updates to the standard configurations for hardware and Core SW. Concurrently with these updates, hardware equipment due for tech refresh shall be scheduled for refresh.
- **Ongoing Updates.** Ongoing incremental, regular updates to approved configurations. Ongoing updates shall relate primarily to software.
- **Emergency Pushes.** Event-driven, defensive security pushes to protect the security posture of the standard desktop configuration and minor functional updates from the software OEM (versus major version upgrades, which shall be assessed more thoroughly and are part of the standard yearly update).

Contractor shall only perform refresh activities which either 1) have passed the configuration control and governance processes to become part of the standard configuration, including having been assessed for cost/risk/benefit; or 2) are emergency in nature and have been approved through a streamlined process.

Hardware Refresh. Contractor shall have a group dedicated to refresh that shall travel the County, working from the refresh list, focusing on one site at a time to minimize disruption.

Software Refresh – Software/SCCM.

Contractor shall use System Center Configuration Manager (SCCM), previously known as SMS, to automate refreshes and updates and manage the overall deployed configuration. SCCM shall prevent users from installing un-authorized software or authorized software in unauthorized configurations.

Software refresh shall include updates to the OS and applications.

SCCM

Contractor shall provide SCCM 2016 and the following core capabilities for the County:

- Software distribution – by End-User, by machine; mandatory and optional (self-service)
- Asset intelligence – hardware and software inventory, compliance, application usage tracking
- Hardware and software updates – firmware and security updates
- OS deployment – for workstation only
- Mobile device management

SCCM 2016 shall be introduced into the Library environment to maintain currency of and distribute software to the devices on the Library network with the enterprise standard tool.

Using SCCM, non-emergency software refresh shall be performed outside core hours, usually at 2:00 a.m.

Major software and OS version updates (e.g., from Windows 7 to 10) shall be considered changes to the standard configuration and shall be managed as such. For major OS upgrades, the methodology is more extensive and may include re-imaging the disk.

Requests for Change (RFCs) shall be used to document a change to the environment. Updates may be applied as a push change and documentation shall remain in the knowledge repository of the End-User Services. The RFC shall remain in the CRCB document repository.

Contractor shall adhere to the County Microsoft Windows Non Security Updates Process document. Contractor shall follow overall architecture, desktop, and LAN/WAN security practices, using tools described below.

For security-related updates, in addition to the steps above, the security office shall review and validate the security updates. Urgent updates shall be pushed out on an accelerated schedule—either that night or immediately—in accordance with streamlined emergency approval process.

Approaches, processes, and procedures are governed by County procedures.

Operations and Maintenance of Core Software, including OS.

Desktop Engineering shall have procedures for maintaining the OS image and core software. On a quarterly basis, new device drivers shall be tested for items such as printers and network interface cards and added to the OS image. Security and non-security updates shall also be added quarterly to the OS image to facilitate a faster imaging process. Core software shall be updated during the year with minor revisions, to address vulnerability issues with the browser, for example. Major revision upgrades of the Core software and OS shall be addressed via updates of standards that are approved by the County and executed as projects.

Maintaining an up-to-date (Core Software) Desktop Computing environment

Generally, updates to the desktop environment, including hardware, core software and OS, and all other components, shall be organized as:

- **Standard Yearly updates.** These are the annual updates to the standard configurations for hardware and core software. Concurrently with these updates, hardware equipment that is due for tech refresh shall be scheduled for refresh.
- **Ongoing Updates.** This is ongoing incremental regular updates to approved configurations. Ongoing updates shall relate primarily to software.
- **Emergency pushes.** Emergency pushes shall be event driven. Typically, these are defensive security pushes to protect the security posture of the standard desktop configuration and minor functional updates from the software OEM (versus major version upgrades, which are assessed more thoroughly and are part of the standard yearly update).

SCCM.

To maintain the core software configuration, Contractor shall use SCCM (previously SMS) to automate refreshes and updates and manage the overall deployed configuration. In addition, SCCM shall control and identify users installing unauthorized software or authorized software in unauthorized configurations.

The software distribution process shall be as follows:

Software Distribution Process

- The County approves the core software standards and configurations.
- Desktop Engineering (DE) posts completed Software Distribution templates to the DE SCCM Production Requests SharePoint site and informs SCCM Ops.
- The SCCM Ops team lead reviews the document for accuracy or any issues.
  - If issues found, he notifies DE and requests update/correction.
  - If no issues found, he sends notification to the SCCM Ops team and applicable desktop engineers that it is approved for production distribution.
- SCCM Ops team member is assigned to perform the setup in the SCCM console.
- SCCM Ops team member sets up the software distribution as specified in the document.
- SCCM Ops sends notification to SCCM Ops team and applicable desktop engineers that setup is complete and includes details of the setup and a link to the advertisement status report for the new advertisement.
- After the advertisement start/mandatory time, SCCM Ops monitors the advertisement status to help identify and correct problems with distribution.

End-User computer devices shall be locked so users cannot perform their own installs.

Performance or systemic issues on desktops

For enterprise-wide systemic issues in the desktop environment, Contractor shall use ITIL Problem Management to identify the root cause and to drive remediation. Steps shall include:

- Treat performance and systemic issues as cross-functional problems in that they involve desktop services, engineering, asset management, etc.
- Use data from tools (such as Riverbed, Cascade and APM), users, and tickets.
- Perform analytics; look for patterns and trends.
- Isolate a problem or determine a pattern of the same problem, then attempt to replicate the problem in Contractor's test lab so that Contractor can conduct deeper diagnostics.
- Promptly escalate and involve vendor support channels as needed.
- Identify the error and generate RFCs, either to configurations and/or service standards depending on the problem.
- Depending on the nature of the problem and the solution, it may be an emergency push or bundled with a regular release.

- If the root cause of the problem is with the core software configuration, Contractor shall go through the appropriate engineering and testing process to correct the error, gain the County's approval, and change the standard.

At the deskside level, if Contractor finds that there are multiple incidents, or troubling trends, Contractor shall enlist Problem Management to find the root cause and remediate it.

Specific Issues. For any issue, Contractor shall identify it, resolve it, identify the root cause, and then modify standards and/or procedures to prevent the issue from occurring in the future.

Contractor shall have effective processes in place to identify systemic issues that involve human feedback, trouble ticket data analysis, and system performance data. Contractor shall have a rigorous process to promptly address the root cause of systemic issues.

Engineering desktop software and Constant Improvement of quality and timeliness of applications and software package delivery to End-Users.

Service to the User.

Contractor shall involve the End-User and provide the End-User a voice and authority during each phase of Contractor's approach.

Plan

- An End-User shall be able to initiate a request via the Service Portal for new software or applications or support to existing software or applications
- Users, Group IT Managers, CTO, and Contractor Applications team representatives shall be involved in the annual standards refresh along with Enterprise Architecture and Desktop Engineering
- Users, Group IT Manager, CTO and Contractor Applications team representatives shall be involved in the weekly Enterprise Architecture meetings with Desktop Engineering
- Users shall help specify and conduct End-User acceptance testing (UAT)
- Applications shall be tested both by Contractor (first) and the sponsoring End-User

Build

- User manuals, FAQs, and other supporting reference material shall be configured and deployed.
- User feedback from prior similar deployments shall be incorporated

Operate

- User shall receive an introduction deskside to new equipment and software
- Various types of End-User training shall be available depending on the nature of the software and applications
- User service shall always be available via the Service Desk

Desktop Engineering

Requests for packaging software for the desktop shall be made through catalog requests or project requests from the County. As such, Desktop Engineering shall create the installation package, test it in the engineering lab, peer review it, and provide it to the client to conduct UAT, in the case of a catalog request or the Contractor Applications team for testing, in the case of project/portfolio requests. Upon successful Applications team testing, client UAT shall be conducted. When client approval has been obtained, Desktop Engineering shall submit the request to End-User Services – SCCM Ops for production deployment.

Performance Monitoring – HES shall monitor the performance of the applications and hardware devices as part of the overall enterprise. When there is a reason for deep applications performance monitoring or any kind of

additional performance monitoring, Contractor shall perform troubleshooting and analysis using the tools and teams that Contractor discussed previously in this section. The addition of the analytics data warehouse that Contractor puts in place shall pull together the complete view of the information and data that Contractor has within its systems.

Performance Tuning - When applications need tuning, Contractor shall work cooperatively with the application vendor and the Contractor Applications team.

Continuous Improvement

When MASLs identify a process quality issue, Contractor shall implement CSI following the standard Deming Cycle (Plan/Do/Check/Act). Contractor shall on a continual basis seek to improve End-User services by identifying improvement areas, planning and implementing remediated items, and measuring the change in Contractor's quality metrics.

Quality and timeliness of delivery

The quality of desktop performance shall be constantly assessed at many levels.

Quality of Applications. Quality of applications and their hosting shall be tested as the application is approved for the standard configuration or OIPC. In addition to Contractor-performed SIT and UAT, the hosted application shall be tested by the sponsoring End-User. Finally, the applications in the configurations shall be tested by service technicians when an IMAR or refresh action warrants.\

Timeliness of Software Package Delivery.

Contractor shall proactively work throughout the process to facilitate the speed with which users can obtain new applications and the speed with which they can supported. Applications shall go through the Plan, Build, and Operate process.

Plan.

Contractor shall work closely with the County during each step so each application request is prioritized correctly. Contractor shall use the GR, CRB, and weekly Enterprise Architecture review meetings as forums to achieve this. Applications shall be tested both by Contractor (first) and the sponsoring End-User. Some packages require legacy configuration of the standard desktop.

Build.

Once an application is approved, during the Build phase, Contractor shall address engineering issues on a case by case basis and work cooperatively with the application owner.

Operate.

As applications are released as approved and are part of OICP, all standard procedures shall apply. Applications operational issues shall be resolved at the highest possible tier, but some applications are specialized and complex. Applications escalation shall be a Tier 3 item.

4.5. Desktop Computing Services

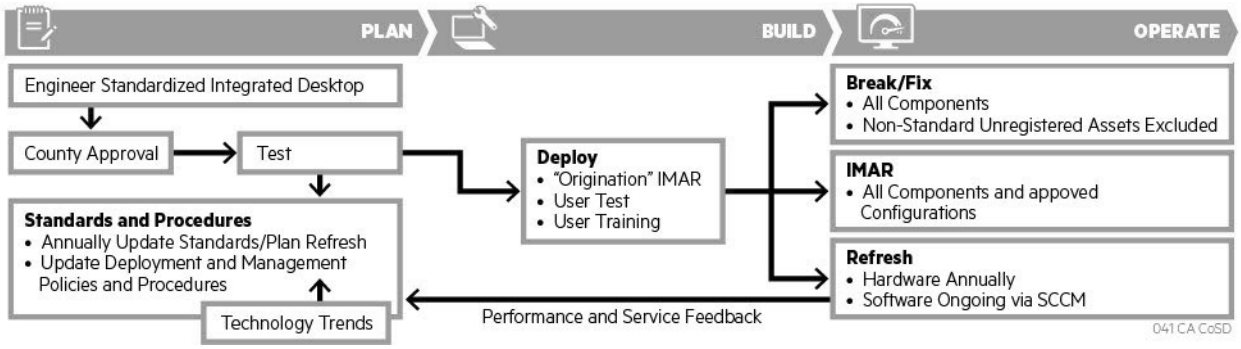
4.5.1. Process and Procedures

- Solution to meet the requirements

Contractor's Desktop Computing Services framework solution shall integrate all required components of End-User Services, interfacing components (such as Service Desk) and cross-functional components (such as Asset Management). The figure below illustrates Contractor's integrated framework.

Contractor shall use the existing framework methods throughout the transition for a smooth and reliable process. The framework shall be driven by the "plan, build, operate" concept, as illustrated in the figure below.

Desktop Computing Services Activities across the Plan, Build, Operate Lifecycle

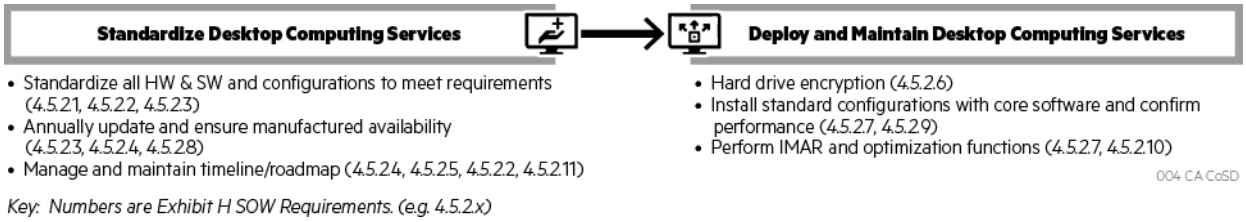


Contractor shall manage the desktop services and architecture as an integrated solution across the Plan, Build, Operate life cycle structure.

Rationale for Choosing This Solution

This solution shall provide standardization as a key component to optimizing service (see figure below). The bulk of Contractor's efforts shall focus on enhancing Contractor's services to the County— best accomplished by standardizing a set of technologies that recognize the diversity of the employee base and also derive support, cost, and efficiency benefits.

Desktop Computing Services Solution



- Deployment plan for resources and use of facilities

Facility Approach. Desktop Computing Services shall provide by a Contractor services team located centrally at Contractor's Rancho Bernardo facility. Additionally, Contractor shall have embedded support technicians at the COC and CAC.

- 1 employee shall reside at the COC
- 2 employees shall reside at the CAC

As service issues require in-person support, Contractor shall deploy technicians from Contractor's regionalized End-User support team. Most site technicians shall reside at Contractor's Rancho Bernardo facility. The technicians shall use this as their home base, traveling to any of the County sites with the equipment and tools required.

Contractor shall staff the core hours of Monday through Friday 6:00 a.m. to 6:00 p.m. with a full shift. Non-core hours shall be staffed at levels sufficient to provide necessary service as required over the weekends, on holidays, and after the business day. Contractor's support service levels shall be available 24x7x365. Online ticket creation shall be available with the Service Desk 24x7 via the Service Portal, phone call, or chat, so even non-urgent service tickets can be logged anytime.

How Desktop Encryption shall be conducted, measured and reported:

1. Conducted: An Contractor recommended, and County approved Standard PC, Standard Laptop and Engineering Workstation Hard Drive Encryption solution, (e.g., Symantec EndPoint Encryption) shall be installed on all Standard PC, Laptop and Engineering Workstation as part of the Core Application Suite prior to delivery to end-users. The approved solution shall be maintained at current vendor version. The Hard Drive Encryption solution shall be installed on all County assets by certified Contractor Services Technicians, or remotely via SCCM. If installed remotely, a successful install shall be verified/QA'd by Contractor prior to deployment and/or turnover to End-User.

2. Measured: The Reporting Console for the Hard Drive Encryption solution shall be the primary tool utilized to identify any Standard PC, Laptop and Engineering Workstation not reporting a successful install of the approved Hard Drive Encryption Solution. Other tools such as SCCM may also be utilized to identify compliant/non-compliant devices. Regularly scheduled electronic scans of all County connected devices in the environment by the Reporting Console shall be the primary tool to measure the quantity of encrypted and non-encrypted devices on the Network. All non-compliant assets shall be scheduled for remediation and/or repair by End User Services.

3. Reported: At requested scheduled intervals, the Reporting Console for the Hard Drive Encryption Solution shall generate a report of all assets by asset tag number that are reporting as compliant and/or non-compliant. The Report shall identify each asset by asset tag and the present version of the Encryption software installed. This report shall be provided to the County and posted on the County Service Portal.

How Desktop Optimization shall be conducted, measured and reported:

1. Conducted: Contractor shall perform optimization analysis daily using Contractor's automated tools that aggregate findings and establish trends that become the basis of Contractor's weekly reporting. Performance issues identified by monitoring or Incident Trending reporting or County escalation shall be investigated by Contractor Problem management team for Root Cause Analysis (RCA). RCA results shall be reviewed and provided to Contractor End User Services Engineering. Contractor End User Engineering shall identify and test solutions to resolve RCA findings and provide those findings to Enterprise Architecture.

2. Measured: Frequency and duration of issues shall be measured by Incidents reported in the HPSM tool.

3. Reported: Contractor shall report issues, findings and resolutions to the County and post on the Service Portal.

How Desktop Performance shall be conducted, measured and reported:

1. Conducted: Formal Desktop Hardware and Software Standards shall be reviewed annually to ensure that the Core Applications suites approved for the County are implemented. Contractor recommended changes to Hardware Standards and Software Standards (e.g. New and or modified existing Resource Units; updated Core SW Versions) shall be tested by Contractor for compatibility, functionality, and performance with the existing approved Core Software suite.

2. Measured: Performance shall be measured by tools such as Cascade and the Application Performance Management suite.

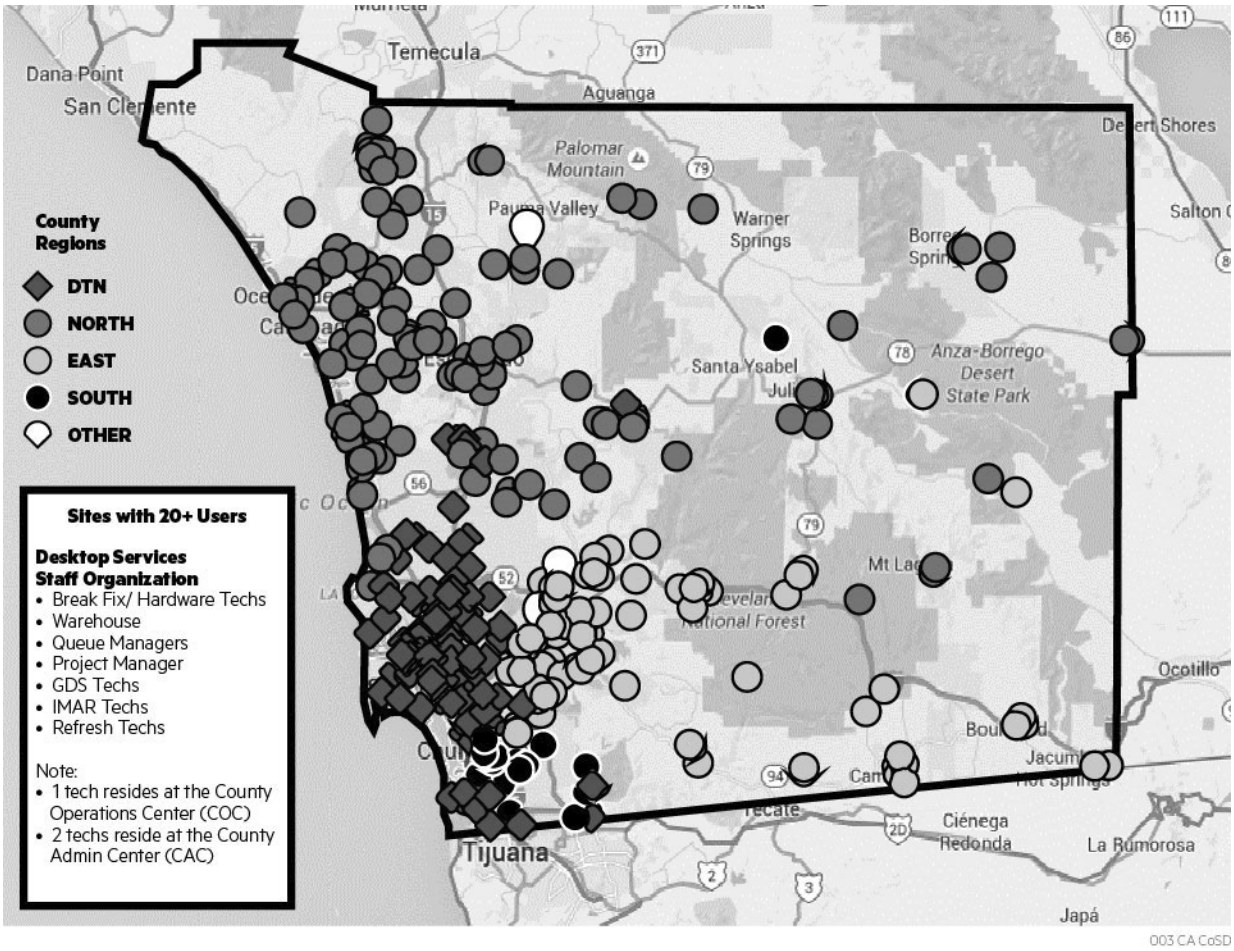
3. Reported: Monthly Reports shall be provided to the County and posted on the Service Portal.

Service Management. To serve all the sites that do not have dedicated onsite support, Contractor shall have a functionally organized technical support team. This team shall travel in a fleet of vehicles, each of which is provisioned with spare parts and "hot swap" spares to provide "first-touch" issue resolution where possible. After assessing the problem, Contractor's technicians shall have the necessary troubleshooting skills and shall be empowered to restore End-User service quickly. Contractor shall then take the faulty equipment back to the warehouse for more extended diagnostics and repair.

Service Scheduling. Service technicians shall provide numerous types of service, including break/fix ticket requests, IMAR actions, or software refresh. Hardware and core software configuration refresh actions shall be planned for implementation throughout the year. IMARs shall also be planned in advance and are non-emergency. For event-driven break/fix service, technicians shall be deployed by the queue manager based on the functional content of the ticket and the End-User's location. The figure below shows the geographic coverage of End-User support and summarizes the functional organization of End-User Services.

Emergency Management. In the event of a disaster or emergency, the Desktop Computing Services team, along with the framework teams, shall provide immediate services to the County. When the OES is activated, the service delivery manager (SDM) on call, along with the Infrastructure Operations Manager, shall immediately be dispatched to the County location with a desktop technician to provide the first shift of support. Contractor shall have a robust rotation of management and technicians that shall remain on site with County staff and other entities that are brought in to support the effort.

Functional and Geographic Organization of Service Staff



When these events occur, Contractor shall work with the County to stand up Local Assistance Centers (LACs) strategically placed where the event has occurred. Contractor, along with AT&T, shall provide all the equipment, connectivity, and onsite staff to offer County employees everything they require. If the OES is not activated and a request comes in from a business group to provide support for a disaster, Contractor shall implement the same process and provide the same support.

Service Technician Skill Profile. The minimum skills and experience required for all technicians shall be as follows:

- Desktop OS (Windows 7, Windows 8.1), with mandatory Windows 10 training for all techs underway
- Basic level server hardware replacement skills
- Customer service skills
- Basic data backup skills
- Minimum 2-year remote and onsite troubleshooting experience
- Attention to detail
- Deskside End-User and technical communication skills

All technicians shall have the same base skills and shall be cross-trained so that, in periods of surge, Contractor can meet the service demand.

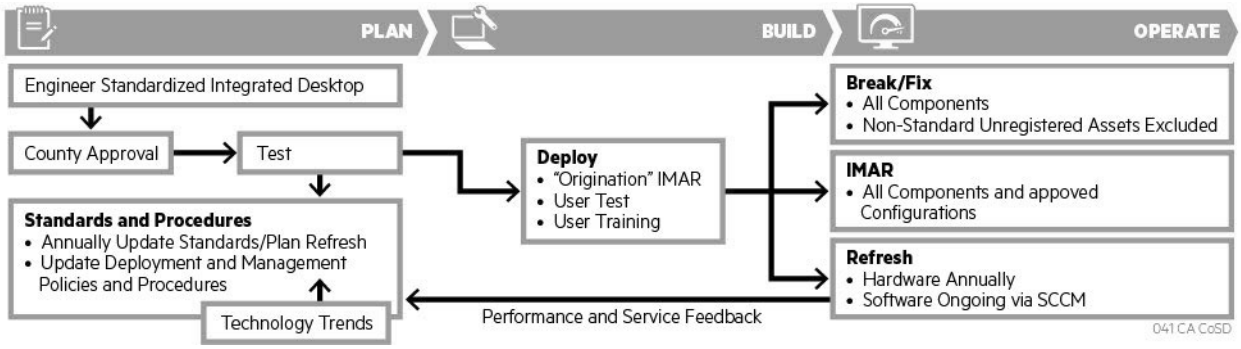
In addition, Contractor shall provide communications to Contractor's service technicians to keep them up to date on the County's mission via all-hands meetings, webinars, leadership briefings, weekly/monthly newsletters, knowledge shares, and other County specific activities.

Contractor's service technicians shall be aware of Contractor and industry state-of-the-art and best practices via newsletters, webinars, the internal Contractor portal, team meetings, and so forth, for information about the latest technology, and for continuing education.

- Key methodologies and processes in solution including year-to-year continuous improvement

The following figure shall serve as a roadmap for Contractor's Desktop Services Methodology.

Desktop Services Methodology



The **Plan Phase** shall include engineering, testing, establishing standards for desktop hardware and software, and obtaining applications approvals. The standard desktop configurations shall be re-assessed and updated annually with County review and approval. During this annual review, the technology may or may not change. Update decisions shall depend on complexity, End-User benefit, technical necessity, and County approvals. Contractor shall continue to bring full transparency and engineering rigor and review into the annual update process. The Optional Items Catalog (OIC) shall include non-standard items that the End-User may still require. In addition to supporting the current field equipment, the standards engineering function shall also include forward-looking work with vendors and the greater technology community to anticipate and plan for future incremental and transformative configurations. These shall be documented in the timeline/roadmap documentation and briefing to the County annually.

The Desktop Engineering organization shall maintain, update, test, and annually release the standard hardware and software configurations. Desktop Engineering shall work with Enterprise Architecture to integrate into the environment, and provide cross-training to the Operations team. This group shall coordinate engineering and testing prior to deployment to address and eliminate issues such as older drivers and network interface card (NIC) mismatches.

Contractor shall conduct a weekly Infrastructure Project meeting to discuss the current status of ongoing infrastructure-related projects in the environment. Enterprise Architecture meetings review, for example, new technologies, changes to the desktop hardware and software standard and technical requirements for a project.

The **Build Phase** shall include the full set of activities to assemble, deploy, and test each individual standardized unit (with approved options); these shall include desktops, laptops, tablets, printers, and other network resources in a standardized MS-Windows based environment. Contractor shall follow the following process:

- Upon receipt of the hardware, Contractor shall tag it and have it ready for imaging when needed.
- The machine shall be pulled from the warehouse, and prepared to be imaged based on the configuration requested.

- Once the image/applications are completed, validated, and tested, Contractor shall put the equipment in the warehouse, where it is kitted with all of the accessories, and shall ensure the device is ready for delivery.
- Service ticket documentation or communication from the refresh the project manager shall then tell the technician where and to whom to deliver the hardware.

Desktop Engineering shall create a custom enterprise operating system (OS) image for the County, which shall comprise the MS Windows operating system and device drivers. This custom OS shall be made available to the imaging technician who handles imaging for refresh, IMAR, break/fix. During the business day, Contractor shall have staff onsite in the Rancho Bernardo facility in the imaging room that can complete hot swap devices for loaners as needed, and copies of these images shall be provided to the technicians in the field for onsite re-imaging.

The **Operate Phase** shall include the maintenance, operations, refresh, IMAR, break/fix, and everything else to support daily operations for the End-User. Operations and support activities shall cut across the frameworks and integrate User Service functions from the Service Desk, such as ticketing and remote support; service management functions such as asset management, configuration management, and process improvement; and other components of the End-User Services framework. Generally, Contractor shall adhere to the following process:

- Ticket requesting action shall be received, logged, and dispatched to a technician.
- Technician shall perform the required action to resolve the End-User's issue in accordance with documented procedures and services standards.
- Functional operation of the hardware and/or software shall be validated by the technician before permission is obtained from the End-User to close the ticket
- User satisfaction shall be confirmed verbally and via the Customer Service Survey sent out at the closure of the ticket.
- Asset management database shall be updated, if required
- The ticket shall be closed.

Hardware and software not in the standard configurations, such as BYOD smartphones and standalone printers, shall be supported as non-standard items. Contractor shall have processes in place to support requests for service on these items on an as-requested basis.

The Desktop Computing Services component shall be used to integrate all components of the desktop configurations: hardware, software, applications, network print, communications and, MDM.

Scheduling

For the annual refresh requirements and schedule, Contractor shall make all reasonable efforts to complete all the equipment at a given location before moving to the next site. Communications shall go out at multiple points for each device to prepare the users and avoid as much disruption as possible on the day of refresh. A target schedule shall be provided on an annual basis to the identified points of contact (POCs) to review and make edits as needed. Contractor shall work with the County's IT coordinators directly, along with the CTO point of contact, so that if changes need to be made to locations and dates, Contractor can accommodate them to prevent disruption. Contractor shall have a dedicated project manager assigned to the refresh activities of the End-User devices to provide solid communication, consistency, accuracy, and delivery of services in this space. The project manager shall also be responsible for the overall status of the project plan created annually for each refresh cycle and shall report on that weekly in the Infrastructure Project meeting.

Refresh.

Technical refresh shall be performed on a rolling basis throughout the year based on equipment type, install date, and refresh timelines. There shall be a 6-month refresh availability window that shall start 6 months before the

scheduled refresh date and a 2-month grace period after each refresh date. Contractor shall take these into account during refresh planning and optimization. Contractor may exceed the 6-month early refresh window based on County requirements.

In addition, the County may request an early refresh of a desktop computing asset through the IMAR process at any time out of normal refresh cycle. If the device is not in the current refresh schedule or the request date is greater than 6 months earlier than the normal cycle refresh date, the department shall be charged a pre-defined rate per month based on device type.

Desktop Computing Services shall have a team of refresh technicians who specialize in performing refreshes. The technical refresh process shall be as follows:

- At the beginning of the calendar year, a draft schedule shall be communicated to the County
- Contractor shall work with the County to around any County business events. Contractor shall then finalize the schedule with the County coordinator.
- Prior to performing planned work at a site, Contractor shall communicate with the coordinator to validate planned activity is still acceptable.
- A review of every device shall be completed 3 to 4 weeks in advance of the actual refresh to identify custom configurations, applications, standalone hardware requirements, replacement model, extra tray requirements, and so forth.
- Equipment, including software configurations, shall be prepared to the extent possible at the warehouse prior to delivery to the End-User based on the information from the pre-field form. This shall include hardware configuration, any hardware default settings, basic software imaging, and standard software configurations.
- Testing is performed.
- Communications shall be sent to End-Users and POCs during all required steps of this process to make certain that nothing is missed.

At the End-User site, Contractor shall back up configurations from the machine that is going to be replaced. Users shall be notified during pre-communication to move data off the devices and onto shared data locations. The technician shall transfer any data that resides on the device that is related to applications. The technician shall also offer up to 30 minutes his or her time to transfer data unrelated to applications as a part of the refresh scope of work. The following actions shall be performed by the refresh technician at the End-User's site:

- Disconnect existing hardware, noting and/or tagging anything End-User- or site-specific, unique or non-standard.
- Install new hardware in the standard configuration, noting and addressing anything End-User-specific.
- Restore End-User configurations onto the new equipment; re-establish network access and network configurations.
- Perform functional tests to demonstrate to the End-User that the refresh was successful. Troubleshoot any issues.
- Make the End-User aware of any new features/functions of the new configuration and equipment. Point the End-User to relevant frequently asked questions (FAQs) or training, if needed.
- Notify the refresh project manager that the refresh is complete.
- The refresh project manager updates the database and reporting measures as activities are confirmed completed by the technicians.
- Notify the Service Desk that the ticket is complete.

In addition to desktop hardware refresh, there shall be an ongoing stream of major and minor software updates. These updates shall be managed by SCCM and shall usually be automatic and transparent to the End-User.

Break / Fix / Hardware Technical Support

Break/fix services shall be event driven and triggered by a service ticket. Technicians shall manage service on the integrated desktop configuration, not just the hardware.

Queue Management. Within Desktop Services, the queue manager shall assign tickets to technicians. This function shall be performed via a process supported by MS Office tools for scheduling. Technicians shall be assigned in an optimal manner, based on a combination of technical requirements, urgency of the ticket, geography of the ticket, and the technical complexity of the problem. For High Response End-User service, Contractor shall make all reasonable efforts to assign a familiar and experienced technician the High Response End-User knows and trusts. When a problem requires desk-side support, Contractor shall use the following methodology:

- Ticket forwarded from Service Desk to queue manager
- Queue manager determines to whom to assign the ticket
- Ticket is assigned to a technician, and the technician is notified of the ticket assignment
- Technician travels to End-User and performs the appropriate diagnostic protocol for the identified problem

To diagnose the issue, generally technicians shall use tools such as HP Diagnostics Toolset, LogMeIn Rescue, SCCM, Active Directory (AD), MS OffCAT, AirWatch, and others, depending on the nature of the problem. Technicians shall have additional options available for more complex problems:

- Correct the problem at the deskside using break/fix troubleshooting procedures for the specific problem
- Get peer level technical specialist support to assist with problem resolution
- Escalate to a SME as appropriate
- Hot swap to a loaner
- Hot swap to a spare

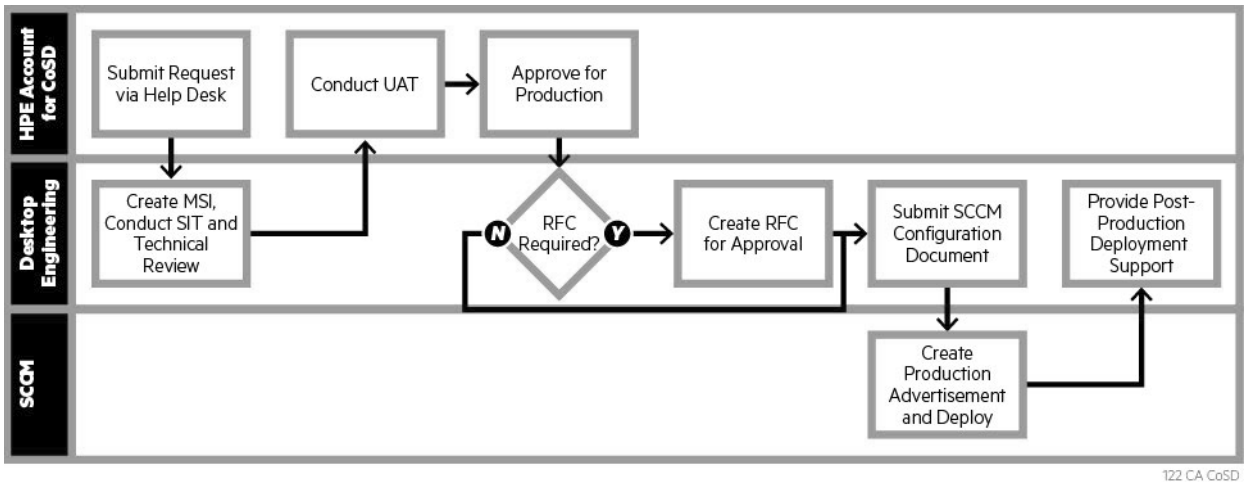
Technicians shall select the right method to get the End-User back in service as quickly as possible while still resolving the root-cause technical issue. The technician shall test and demonstrate to the End-User that the problem is fixed.

- The technician shall perform the foundational set of system and End-User testing, which is a series of standard tests.
- Technician shall log the fix, update the asset inventory (if necessary).
- Upon completion of the service, the technician shall move on to work their next ticket

IMAR

IMAR requests shall typically be triggered by non-urgent events. Any IMAR request that comes in with more than 25 items shall be considered a project and assigned within the End-User Service group to the project coordinator to manage and complete as required. The IMAR process flow, illustrated in the figure below, shall be the same as for all other types of requests.

IMAR Process



HPE Asset Manager shall track all modifications to an asset record that are the result of moves (locations, users, and so on), adds (adding components), or changes (any other changes to the asset record). Modifications shall be tracked by field. If a field value is changed, HPE Asset Manager shall capture the name of the person making the change, the date of the change, and the name of the field that has been changed as well as the previous field value.

Moves, adds, or changes to assets can also be discovered or confirmed through auto-discovery, using the DDMi (Discovery and Dependency Mapping Inventory) tool for consistency. Contractor shall also provide tools to automate software-related IMAR activities, including policy-based software management. An IMAR action can be for a complete desktop, laptop, or other device configuration or just a component. Overall, the IMAR process shall be as follows:

- Receive an IMAR ticket
- Travel to the site of the equipment/bring equipment to the site location for install
- If the equipment is onsite, complete the identification and validation of this equipment to make sure inventory numbers match the tickets and asset database
- Back up all relevant End-User data and configurations and other environmental settings if required
- Make the appropriate IMAR action as indicated in the request:
  - **Install.** The "origination IMAR" is a special case of installation. For the first installation, the equipment is new, newly refurbished, or wiped to a new configuration. Where Contractor is able, new configurations of equipment can be prepared in the warehouse with hardware configuration, the standard software image installed, and any End-User optional items installed. This preparation work shall ease the installation process at the End-User's desk. Then configuration to the End-User's environment—for example, preferences, network connectivity and printer connectivity—shall be completed.
  - **Move.** A move is similar to a remove and install, except that software installation does not need to be performed. For a move, the technician shall note the End-User's connections and configurations, power down the old equipment, minimize its disassembly but do enough disassembly to safely move the equipment, and then physically move the equipment to the new location. Once at the new location, the technician shall perform the necessary installation steps completing with reconfiguration of End-User-specific and site-specific parameters.
  - **Add.** An add is typically for a new piece of hardware or software. Procedurally, an add follows the same steps as an install.
  - **Remove.** Complete removal of equipment can happen when an End-User leaves the County or when the equipment they are using is refreshed. Upon removal, the technician shall shut down the equipment, making necessary logical and physical disconnections and take the equipment away. Removed equipment shall go through the warehouse for asset management and proper disposal. Hardware at end of life shall

be so noted in the asset management database and is donated to San Diego Futures Foundation (SDFF). Removals of software shall include an action to make certain that any active licenses that were originally obtained are returned to the licensing pool for reuse.

IMAR Testing. In all actions that result in retained or upgraded equipment, the technician shall validate via deskside testing that the End-User functionality is correct and End-User configurations are created and/or retained as appropriate. This deskside test process shall be similar to that described in break/fix.

Continuous Improvement.

- Using the Deming PDCA (Plan/Do/Check/Act), Contractor shall on a continuing basis seek to improve End-User Services by finding improvement areas, planning remediation and implementing them, and measuring the change in Contractor's quality metrics.
- Contractor's leading indicators of quality shall be the service levels measuring Contractor's performance along with the Customer Satisfaction Survey data provided. The service levels and surveys are leading indicators of quality, but Contractor also has all the data and analytics about the installed configurations and break/fix trends such as types of tickets, hardware configurations involved, system performance to ensure maximum optimization of the desktop environment, the nature of problems, and time to repair metrics.
- Contractor shall analyze these indicators to determine if Contractor needs to embark on a Service Improvement Plan to improve Contractor's quality. These efforts shall be tracked, and the team recommends improvements. After putting them in place, Contractor shall then monitor closely both the incident and problem trends and their impact on Contractor's service level performance.

During the Cross-Functional Transition, Contractor shall implement Microsoft SQL Server Business Intelligence to begin the process of building a reporting data warehouse, thereby bringing more automation and continuous improvement to the reporting process.

While the initial focus is on supporting SLA Reporting, the data warehouse shall provide a central repository that can support other ITSM analytic scenarios. Contractor is committed to continuous improvement and, over time, Contractor shall work with the County to extend both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. Benefits to the County can be measured through increased system availability, reduced system disruptions, predictive analysis of system changes, and optimizing staffing levels.

The four specific areas of focus shall be:

- Service Strategy and Improvement Analytics: This area shall focus on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis

- Service Design Analytics: This is a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data Contractor can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.

- Service Operations Analytics: Blending ITSM data and benchmark IT performance data, Contractor can conduct analysis to reduce business impact of events, incidents, and problems.

- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

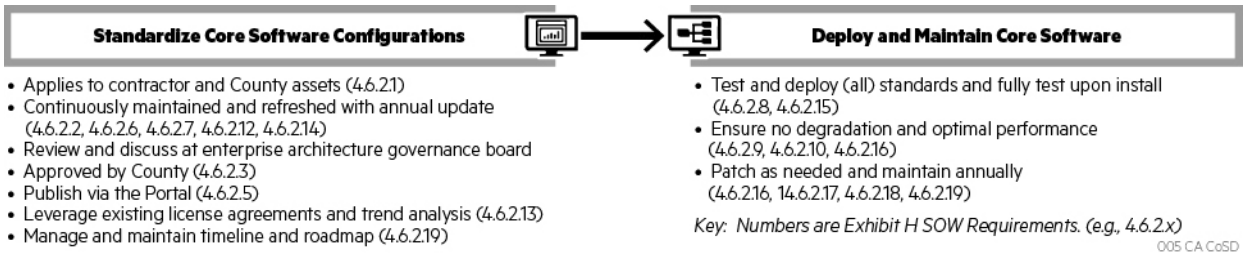
4.6. Core Software Services

4.6.1. Process and Procedures

- Description of solution to meet the requirements

Core Software Services shall be responsible for standardizing, describing, deploying and supporting a standardized and fully tested image onto all desktop assets including county retained assets. The fundamental activities of Core Software Services can be described as Standardization Management activities and Deployment and Maintenance Support activities, as shown in the figure below.

Core Software Service Solution



Core software configuration and updates shall undergo component testing, System Integration Test (SIT), regression testing, and User Acceptance testing (UAT) by the Contractor Technology Office, Applications Office, and Desktop Services organizations. Testing shall be both technically focused and End-User "use-case" focused. Testing shall also validate the security strength and integrity of the core software configuration and install.

Standards Enforcement and Exceptions.

Contractor shall use a process to regularly verify software versions and update as needed using SCCM, which shall scan the installed base of equipment for unauthorized programs. These checks and software updates shall be performed automatically over the network during off-hours.

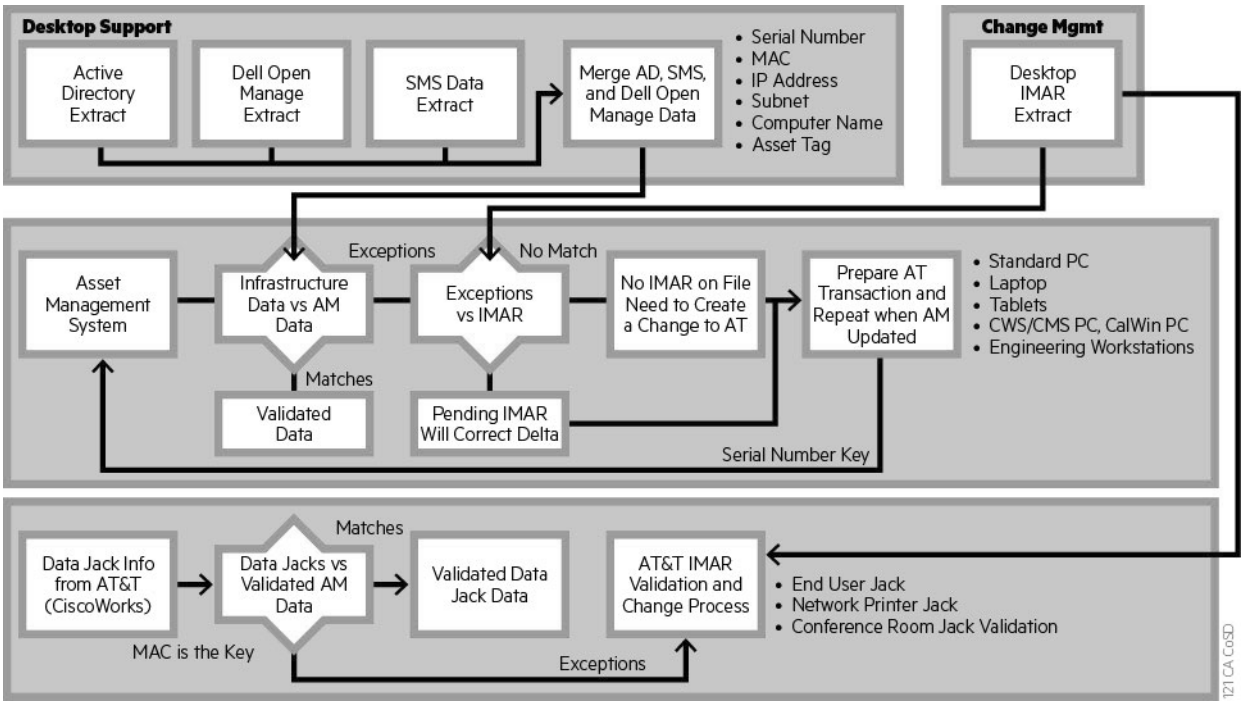
Contractor shall maintain a request process and adjudication process for non-standard items. The standard test shall be whether a business function cannot be performed with the standard configuration—not just that the End-User prefers a different tool. Users shall have FAQs, training, videos, and other tools available to them from the Service Portal to help them learn standardized tools. The End-User Services Manager along with the Service Desk Manager shall ensure all FAQ's and documentation related to the End-User environment is kept up to date on the portal and that as new applications and hardware are implemented the appropriate documentation is put in place as required.

- Deployment plan for resources and use of facilities

The Resource and Facility approach shall be the same as for Desktop Computing Services. In addition to the Desktop Service Technicians, this component shall rely on the Project Management Office, Desktop Engineering, and Testing teams. These people shall also be located at Contractor's Rancho Bernardo facility.

- Key methodologies and processes in solution including year-to-year continuous improvement

Core Software Services Process Flow



Core Software Services shall follow a process similar to Desktop Computing Services (Plan/Build/Operate), as described above. Some aspects with unique characteristic are described as follows.

Integration and User Acceptance Testing. This function shall be performed by the desktop engineering team, using onsite lab devices. This lab shall have access to the County and Library networks, and shall have many device types including the current standards and approved exceptions. When a new custom OS image or a new software package is built, testing shall be performed in this lab via a peer review process—meaning another member of the Desktop Engineering team shall perform the test to make sure it installs correctly, without errors, etc., and provides feedback/results to the desktop engineer who created the custom OS image or software package. Upon successful integration testing, if this is a Portfolio application, the Contractor Application team shall be engaged to perform UAT. When Application team UAT is completed, the software application shall be provided to a small subset of County employees, who perform UAT as well. Upon successful completion of UAT, the software package shall be made available for production distribution to the intended End-User community via SCCM. If this is a catalog application, the County client who requested the application shall perform UAT and, upon approval, it shall be made available to the intended End-User community. If this is a custom OS image, upon successful SIT, the image shall be made available to the support teams via Microsoft Development Toolkit (MDT).

Desktop Computing Refresh – Software/SCCM. System Center Configuration Manager (SCCM) shall be used to automate distribution of updates and to manage the overall deployed configuration. In addition, SCCM shall control and prevent users from installing unauthorized software or authorized software in unauthorized configurations.

Software refresh shall include updates to the OS and applications.

OS refreshes shall be treated as projects and are architected for little to no interruption in the County employee's daily work.

Using SCCM, non-emergency software updates shall be performed outside core hours, usually at 2:00 a.m.

For large OS upgrades within the year on a specific desktop, the software refresh methodology is more extensive and may include re-imaging the disk. Whenever possible, Contractor shall make reasonable efforts to bundle major software upgrades concurrently with hardware refresh equipment replacement as part of the annual cycle to minimize disruption to the End-User's work environment. Security Services for End-User Services shall be based on the defense-in-depth model.

4.7. County Retained Assets Services

4.7.1. Process and Procedures

- Description of solution to meet the requirements

County assets shall adhere to the same standards for configuration of hardware and software as all other assets. These machines shall be verified and enrolled just as all other assets. Then, County Retained Assets shall be serviced and supported using the same strategies, methodologies, procedures, resources, and facilities as contractor-provided assets. All appropriate service levels shall apply to standardized County Retained Asset Services.

When an End-User requests support on a non-standard item or non-enrolled item, the Service Desk or End-User support technician shall identify this situation using the asset database. If Contractor can support the non-standard item easily, Contractor shall do so as an act of immediate customer service on a case-by-case basis, with County approval.

- Deployment plan for resources and use of facilities

Since County Retained Assets that adhere to the standards and are enrolled are serviced the same as contractor-owned assets, the resource and facility approach to servicing these assets shall be the same as it is for Desktop Computing Services and Core Software Services.

- Key methodologies and processes in solution including year-to-year continuous improvement

County Retained Assets shall be managed the same as other assets and the solutions, methodologies, and procedures described elsewhere in this framework shall apply, depending on the nature of the required services.

County assets must adhere to the standard configurations, be "enrolled" to be on record as part of the managed configuration, and be recorded in the asset database. When contractor support is required to "build" the software configuration for County assets, this function shall be performed using the same standards and procedures as described in Desktop Services and Core Software Services. Once a standardized County Retained Asset is successfully enrolled, it shall be managed and serviced such as any other asset. Service tickets shall be flagged as "County Retained Assets" so that the technician knows of the hardware status just in case there is a troubleshooting problem related to the asset's origin.

Enrollment. In order to be serviced, a County Retained Asset must be enrolled in the Service Manager (SM) asset management database. At the time of enrollment, adherence to configuration standards shall be confirmed. Enrollment of County Retained Assets shall always verify by the Service Desk upon first service request.

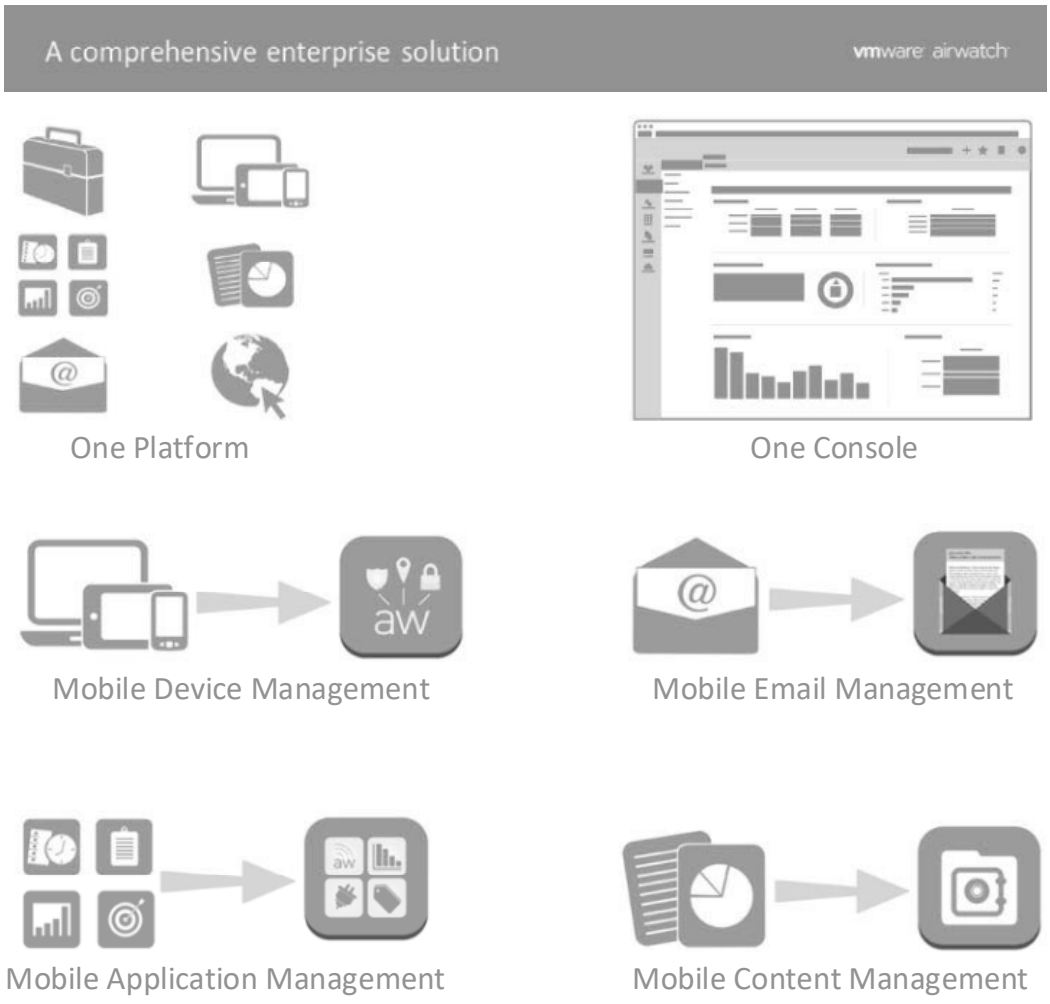
4.8. Mobile Device Support Services

4.8.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide the specific capabilities offered by the AirWatch platform, as shown in the figure below. All initial enrollment and other support requests shall be made to the Contractor Service Desk. The Service Desk shall validate the End-User's information and offer information and support that may solve the problem. For all mobile services that require AT&T support, the End-User's ticket shall get a "warm handoff" to the AT&T helpdesk. Contractor shall ensure that AT&T's helpdesk provides a single AT&T point of contact through each service transaction, even when AT&T needs to access multiple support organizations. Contractor shall ensure that AT&T support handles certain issues either by the local AT&T Incident/IMAR managers or by the AT&T Mobility Solution Services (MSS) and AirWatch partners. These End-User requests shall include Device Enrollment or Registration, Passcode Reset/Unlock, Lock Device, Locate/Find, Add/Delete Users, Device Enrollment (bulk or individual), and Device Wipe.

Capabilities Managed by the AirWatch MDM Solution



To expand support, Contractor shall provide a fully managed Mobile Device Support Service that shall provide comprehensive operational support of all County-provided mobile devices as well as County resources that are available on BYOD devices. This service shall provide County users with single point of contact for AT&T's MDM support, using a multi-tiered model designed to handle any type of mobility support need—mobile application, operating system, content management, device familiarity, email access, and even carrier related issues. The Contractor shall ensure that AT&T Enterprise Mobile Support team resolves AirWatch MDM, device/OS, and carrier-agnostic mobility issues in response to County End-User-generated trouble tickets logged with the Contractor Service Desk. This team shall provide expertise and support for most current mobile devices and accessories and shall directly engage the End-User in the diagnosis and resolution of their issues or shall route requests to the appropriate support organization if required. They shall also provide a "warm transfer" for County users for those issues requiring wireless carrier intervention. Throughout the process, this team shall also provide ticket management and communications through the Contractor's Service Portal so that service levels are accurately tracked and the End-User is kept informed of the status of the request throughout its lifecycle. If the ticket requires further technical intervention, it shall be escalated through additional tiers of MDM support by AT&T.

The following is a summary view of each group's responsibilities:

AT&T Enterprise Mobile Support Team

This group shall interact directly with the End-User on all MDM-related issues and provide the basic support and continuity of support for issues such as Device Enrollment, Device Lock and Wipe, etc. Additionally, this team shall provide general device and operating system support as well as facilitate warm transfer to the carrier as the need is identified. For the large percentage of issues, they shall provide first-call resolution. For the remainder of these tickets, they shall also act as the coordinator for the report if it requires escalation to one of the technical support organizations.

AT&T LCM Trade Street Service Desk

This group shall maintain overall responsibility for ticket management and service level attainment for MDM actions. As part of the ticket flow, they shall also provide the interface to Contractor for custom mobile application support, Active Directory, and Outlook email Exchange group issues.

AT&T Mobility Solutions Services (MSS) Application Service Desk

This Application Service Desk shall provide leveraged technical support to AT&T Enterprise Mobile Support team via phone, email, or internal AT&T portal for additional MDM support services. Responsibilities shall include advanced troubleshooting, isolation and resolution, application use, and configuration support as well as MDM managed services requests.

AT&T ASD/MSS Service Assurance Team

This is the first-level technical escalation point to the AT&T MSS Application Helpdesk, which shall perform deeper troubleshooting to reproduce, isolate, and resolve the most complex technical issues.

AT&T ASD/MSS and AirWatch Mobility Consultant Teams

This team shall serve as the escalation point for the AT&T ASD/MSS Service Assurance Team, which shall involve the AirWatch vendor technical team for any MDM application issues requiring the highest level of analysis and support.

The following figure provides more detail on the organizational roles for the mobile solution.

MDM Support Model

<table>
<tr><td>HPE Service Desk</td><td>AT&T LCM Trade Street Service Desk</td><td>AT&T ASD/MSS and Airwatch Team</td><td colspan="2">• The escalation point for the AT&T MDM SA team for any MDM application issues the SA team was unable to resolve</td></tr>
<tr><td rowspan="3">End-to-End Ticket Oversight</td><td rowspan="2">Overall Responsibility for service assurance on mobility report</td><td>AT&T ASD/MSS Service Assurance Team</td><td colspan="2">• Services Assurance is the escalation point to the Tier 2 AT&T MDM ASD
• Perform deeper technical troubleshooting to reproduce, isolate, and resolve the most complex technical issues</td></tr>
<tr><td>AT&T ASD/MSS Application Service Team</td><td>• Provides helpdesk-to-helpdesk support via phone, email, or web portal for MDM services
• Respnsibilities include advanced troubleshooting, isolation, and resolution, ticket management, and communication, application use, and configuration support as well as MDM
• Enhancement requests
• Send SMS, email, or push messages
• Block Email access
• Passcode reset, lock/unlock, verify device enrollment, and policy verification</td><td>• Add/delete users
• View and verify policies
• View device inventory and details
• Device enrollment
• Verify device enrollment
• Change device ownership
• Events and notifications creation/change
• Relay status back to tier 1</td></tr>
<tr><td>Also interfaces to HPES for custom app support, active directory, and email exchange group issues</td><td>AT&T Enterprise Mobile Support Team</td><td>• Multi-carrier mobility helpdesk, reduces burden on IT staff
• Service and expertise
• English-language technical support
• Single point of contract via phone or email for end users
• Support for most popular mobile device hardware, accessories, and operating system
• Domestic carrier connectivity support via warm transfer or a direct call if preauthorized by the customer
• Application issues triage and referral if necessary
• Verification of email settings</td><td>• Resolution of simple MDM issues such as passcode reset, lock/ unlock, verifiy device enrollment, and policy verification
• Engagement of third-parties for resolution of end-user issues via warm transfer or referral
• Ticket update through resolution</td></tr>
</table>

167 CA CoSD

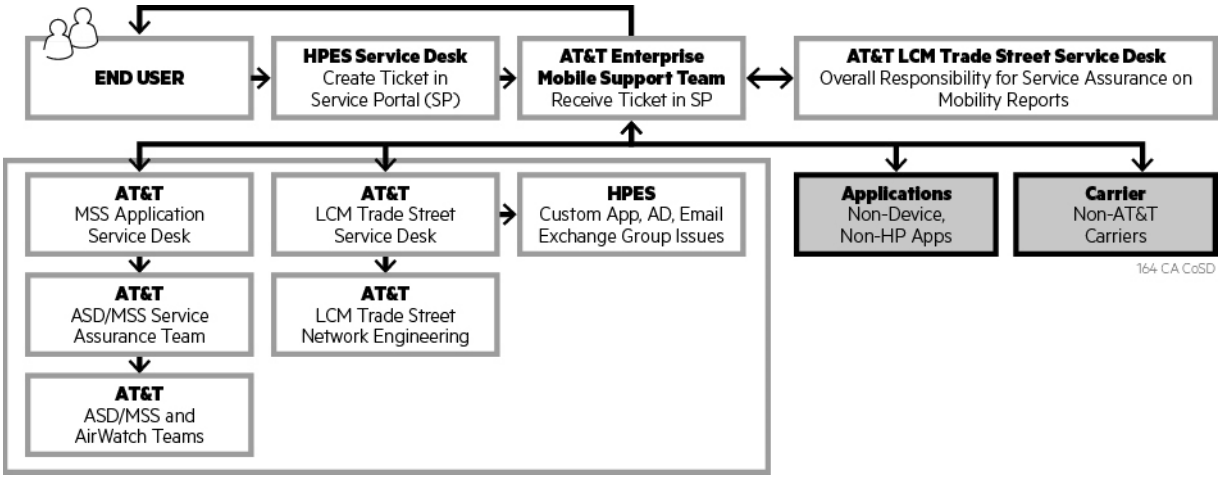
- Deployment plan for resources and use of facilities

Contractor shall leverage the local Life Cycle Management (LCM) team, the AT&T Enterprise Mobility Support team, and the AT&T Application Service Desk (ASD) organization. AT&T LCM personnel shall be located at the AT&T facility in San Diego. All other personnel and facilities shall be located at leveraged sites around the U.S.; this leveraged support shall be transparent to the End-User. The County's MDM infrastructure shall be hosted in the AirWatch shared cloud and shall interface with County resources through a geo-redundant AirWatch Cloud Connector configuration located at both the AT&T Point of Presence (POP) and the County Operations Center (COC). Smartphone users who are using BYOD shall have the option to get additional service related to their devices overall at their service provider's walk-in retail location, including AT&T locations for AT&T subscribers.

- Key methodologies and processes in solution including year-to-year continuous improvement

The same set of tools and processes used by the LCM Incident/IMAR desk shall be replicated for the Enterprise Mobile Support team. They shall have access to the Contractor's Service Desk ticketing platform used for break/fix reports and shall be able to status and resolve tickets generated by the Contractor's Service Desk. They shall also follow existing procedures in using the AirWatch console for MDM related problems. The Contractor's Service Desk Tier 1 agent shall maintain end-to-end ticket tracking, maintaining automated and chat communication with the AT&T Service Desk for MDM, mobile device, and wireless carrier issues. The LCM team shall continue to meet service level responsibilities and shall follow all reports to closure. The following figure illustrates the organization of Service Desk components for mobile users.

County of San Diego Mobile Support Services Methodology



Contractor shall follow the standardized and documented procedures shown in the table below.

Standard Documented Procedures

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
AirWatch – MDM AT&T Incident	Once ticket is received, or warm transfer of caller from Contractor's Service Desk after AD password and role has been verified, Tier 1.5 shall work with the End-User to fix the issue. If Tier 1.5 cannot resolve the issue, it shall be given to Tier 2 to be worked through to conclusion. The incident manager shall document in HPE Service Manager, and transfer the ticket to the correct group to fix the issue or resolve the ticket.	AirWatch Console
AirWatch – MDM AT&T IMAR	Once an IMAR is created, IMAR Manager shall review line item and ensure End-User appears in the AirWatch Portal correctly. Monitor to ensure other line items are closed by Contractor and send out instructions to the requester for AirWatch app install and configuration. Working with End-User on deleting the old device when requested. IMAR manager documents change in the IMAR and close.	AirWatch Console

Remote device management

Remote Desktop Management (RDM)

Contractor shall provide a "warm" transfer escalation process between Service Desk and RDM. If support requests cannot be resolved expeditiously by the Service Desk, then the call shall be escalated to an agent with higher level skills and RDM capability. In some cases, the Service Desk agent shall escalate to a higher tier deskside/field team or technical support. Service desk training and detailed documentation outlining the correct escalation path for each type of incident or service request shall guide agents to make certain that tickets requiring escalation are routed correctly the first time. Contractor shall always ask permission from the End-User before accessing his/her desktop, and the End-User can terminate the remote session at any time.

Remote Desktop Management (RDM). The primary function of the RDM agent shall be to provide a higher level of technical service, handling problems and issues that the first-tier support was unable to resolve and providing RDM skills to increase first-call resolution and customer satisfaction. Using RDM for remote tool capabilities, agents shall remain on the phone with the customer for longer intervals than Service Desk agents to resolve an incident. RDM agents may interact with network services, software systems engineering, and/or applications group to restore service and/or identify and correct the core problem. This may require assisting in simulation and re-creation of End-User problems and recommending system modifications to reduce End-User problems.

Remote Desktop Management agents shall:

- Take tickets routed to them that require a higher level of technical analysis and work these tickets to resolution or route to the appropriate Tier 2 technical support group
- Handle problems and issues that the Service Desk agent is unable to resolve
- Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct a core problem
- Assist in simulation and re-creation of End-User problems
- Recommend systems modifications to reduce End-User problems
- Use LogMeIn Rescue as Contractor's remote desktop management tool.

2.7.6 County managed mobile devices.

For County-managed mobile devices (e.g., handheld devices, smartphones, tablets, and other County retained mobile assets), the methodology for MDM shall apply. Any device that is "County managed" and outside the scope of RU fixed price support requires T&M support.

Contractor shall mitigate against risks such as device loss, data loss or breach, and exposure to malware by using inherent capabilities of the AirWatch client.

Through AT&T, Contractor shall enable secure, VPN-based interaction with enterprise data using one of two methods. First, the Pulse Secure mobile client shall allow applications to establish an encrypted connection to the enterprise via the same SSL VPN solution used for enterprise computing. Second, the AirWatch solution shall allow applications to be developed to use "per-application VPN."

Contractor shall enable AirWatch managed content and collaboration features, using the AirWatch Secure Content Locker tool. This tool shall allow for direct access, encrypted access to enterprise data, leveraging containerization capabilities to prevent data transfer to external sources. Secure access to web-based services such as SharePoint shall also be enabled.

4.9. Unified Communications Services

4.9.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide Unified Communications (UC) Services, which shall enable improved collaboration capabilities across each business areas in the County. These UC capabilities shall include O365, Lync/SfB, Mutare Enhanced Voicemail for voicemail to email delivery as well as Avaya's EC500, which extends both internal and external calls to a County End-User's desk and/or a mobile phone provided by the County. UC capabilities shall be delivered to users on their computer, tablet, smartphone, or VoIP handset.

The following table sets forth when Contractor shall provide the specified UC services:

UC Services

AS OF CONTRACT EFFECTIVE DATE	BY THE END OF TRANSITION	TRANSFORMATIONAL (AFTER COUNTY APPROVAL)
• Mutare Voicemail to Email with SST • Avaya IP softphone • Avaya Extension to Cellular • Avaya IP soft phone for agents • Avaya Enterprise Directory Integration	• Avaya Communicator for Lync • Avaya Collaboration Services for Outlook/ Browser/ Microsoft Office	• Avaya Communicator SIP mobile client • Avaya Presence Services

Office 365 Components

Through the County-licensed Microsoft Office 365 cloud offering, which includes Lync/ (Skype for Business), users shall have access to instant messaging, presence, web conferencing, video conferencing, desktop sharing, and interactive whiteboards.

Table 1. Specifies when the County shall receive the various components of O365

MODULE OF O365	AS OF CONTRACT EFFECTIVE DATE	BY END OF TRANSITION	TRANSFORMATIONAL (AFTER COUNTY APPROVAL)
Lync and/or SfB	Y (Lync)	Partial SfB	Full SfB by 2018
OneDrive	Partial	Partial	Integrated
O365 Office Apps	Y	Continued Y	Continued Y
eMail	N	Y	Continued Y
SharePoint Online	N	N	T&M

Avaya Integration with Lync (Skype for Business)

Contractor shall deploy Avaya Communicator for Lync, which shall allow users to move from limited peer-to-peer audio capabilities into conferencing capabilities hosted within the Avaya Enterprise voice network. As UC services progress, desktop web conferencing capabilities shall become fully interoperable with conventional Cisco teleconferencing platforms.

Other UC capabilities to be implemented include using Avaya Communicator for Lync and collaboration services, which shall contain plug-ins for Outlook, and providing complete call control from the Lync or SfB client with the following key features:

- Click to Call On-Net and Off-Net local and long distance calls, using an End-User's computing device, mobile, or desktop telephone set
- Click to Answer incoming calls from Lync or SfB, using an End-User's computing device, mobile, or desktop telephone set
- Search and Click to Call internal and external County contacts from Outlook email
- Screen pop with contact on incoming calls from Outlook contacts.

Speech to Text (STT) Integration

Contractor shall use the Mutare Enhanced Visual Messaging with STT service. This solution shall transcribe an End-User's new voice mail message into text via email along with a .wav attachment or a secure web link for streaming the message to the County End-User email via SMTP relay.

Mobile Unified Communications

Contractor shall leverage the AirWatch SaaS MDM solution for deployment of UC mobile (e.g. Avaya mobile client, Skype for Business) applications to the County of San Diego mobile application store for corporate owned managed devices, as well as, upon approval, employee owned BYOD devices. Once the UC mobile application has been deployed, whether on a corporate managed device or an employee owned BYOD device, Contractor and AT&T shall provide full support of the application and its connectivity and functionality to the systems that provide these UC capabilities.

Through the integration of the AirWatch Mobile Device Management (MDM) and the Symantec Managed PKI solution for deployment of PKI payload profiles, all corporate managed and BYOD mobile devices and users shall be authenticated prior to accessing UC services or resources. This shall allow for County mobile users to take advantage of the Lync/SfB mobile application, which provides presence, instant messaging, and other capabilities while on the go. Additionally, through Avaya's Communicator for Mobile application, users shall be provided with full enterprise telephony functionality from their mobile device, allowing them to make, receive, transfer, and put calls on hold as well as use advanced features such as Active Directory (AD) lookups and presence status from Avaya voice and SfB users. Users shall have Full Call Control in addition to common enterprise voice features, such as:

- Make/receive calls
- Hold/retrieve calls
- Transfer calls
- Multiparty conference calls.

UC Data Sharing

UC data sharing shall also evolve from traditional SharePoint and network file share capabilities to enterprise file sharing and synchronization.

- **Email** – This shall be provided by Contractor for all County employees and shall be migrated to Office 365 Exchange Online during the transition phase of the Agreement.
- **SMS** – Contractor shall provide this feature as part of the mobile device services, and this feature may be provided by the carrier of choice by business unit. This shall be a hosted service and shall be isolated to the business unit and not available to the enterprise.
- **Fax** – Contractor shall provide Local and premise-based fax services either through the Avaya PBX or separate 1 MB lines by AT&T Core, and shall ensure that all are supported by AT&T life cycle management (LCM). Additional fax capabilities shall be offered by Contractor via the Right Fax solution, which shall be integrated with Office 365 Exchange Online. This solution shall provide users with fax to email services.

UC Support

Contractor shall provide front line support as a part of both Contractor's Service Desk Services and End-User Services. Support and training resources shall also be provided through the Service Portal. Contractor shall continue to leverage Contractor's previous Service Desk activities as well as develop, update, and maintain Service Desk scripts and processes for the UC End-User community. Contractor shall post training videos. As with all Contractor's Service Desk activities, Contractor's UC support shall include incident tracking, escalation, and resolution.

Teleworker and Remote User UC

Contractor shall deploy, after County approval, Avaya Communicator integrated UC and voice services clients. These integrated clients shall provide the 2,600+ users, and any future SSL VPN County users, access to a complete, consistent, and rich set of capabilities both on-net and off-net. Avaya Communicator desktop and mobile clients shall be able to operate in both VPN and non-VPN mode to provide remote connectivity. Avaya's Session Border Controller, in conjunction with Client Enablement Services, shall allow users of Avaya communicator clients (desktop or mobile) to operate in SIP (session initiation protocol) mode. Enterprise security standards, such as TLS and SRTP (secure real-time transport protocol) encryption, shall provide effortless access to UC and voice services integration, enabling teleworkers to function as if they are in the office regardless of their location.

Software and Release Management

Contractor's subject matter experts (SMEs) shall subscribe to Avaya's UC integrated client updates, service packages, or version upgrades. These shall be thoroughly reviewed by SMEs for County environment relevancy and tested in a lab environment before production deployment is recommended. This standardized process shall validate production functionality of any recommended new release update, service package, or version upgrade so that the County End-User environment is not disrupted or compromised.

Contractor SMEs shall apply industry standard software release management methodologies to support standard version delivery and consistency across all County users' devices and assets. These standards shall apply to Avaya One X Communicator, Avaya Communicator for Lync/SfB, Avaya Communicator Mobile, Avaya One X Agent, and Avaya Collaboration Services. The same shall apply to any proposed applications that need to be deployed to the County's managed mobile devices via the AirWatch MDM solution.

Contractor shall create, post, and document consistent UC client software packages for all client types.

This process shall integrate with all ITSM processes in place to ensure communication, approval, etc. and full integration with the overall program.

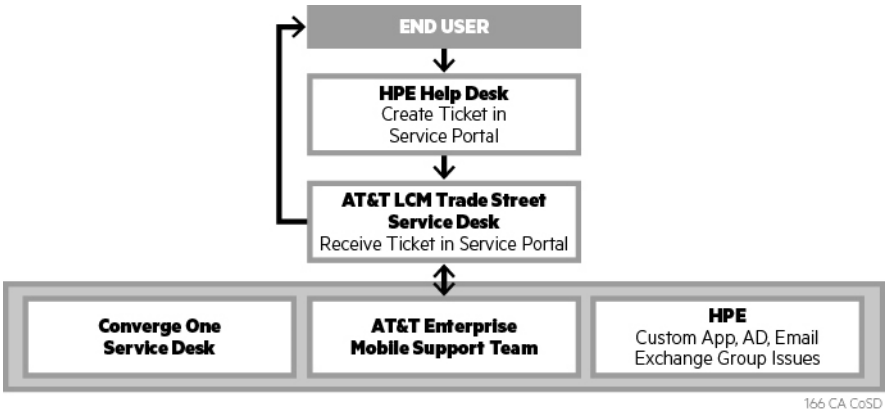
- Deployment plan for resources and use of facilities

As with other services, the County shall use Contractor's Service Desk to support UC. Contractor shall have high-tier support with both AT&T and Microsoft. Contractor's Service Desk shall still own support tickets through the entire life cycle for the convenience of the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

All support services, whether triage, new requests, change requests, or removals shall be initiated by the County End-User to the Contractor Service Desk. All requests that are within the network framework for real/non-real time services shall be directed to the AT&T LCM team for assessment and completion. The following figure illustrates Contractor's support services methodology.

County of San Diego Unified Communications Support Services Methodology



The following table delineates services Contractor shall perform for End-Users in accordance with the standardized and documented procedures.

Services to be Performed by Contractor for End-Users

PROCEDURE NUMBER AND NAME	SOLUTION SUMMARY AND RATIONALE	TOOLS
Mutare EVM Incident Request	Documented process for End-User request to repair trouble with Mutare EVM service	Service Center
Mutare EVM IMAR Request	Documented process for End-User request for active or new service for Mutare EVM	Service Center
Avaya IP Softphone Incident Request	Documented process for End-User request to repair trouble with Avaya IP Softphone service	Service Manager
Avaya IP Softphone IMAR Request	Documented process for End-User request for active or new service for Avaya IP Softphone	Service Manager
Avaya Extension to Cellular Incident Request	Documented process for End-User request to repair trouble with Avaya Extension to Cellular service	Service Manager
Avaya Extension to Cellular IMAR Request	Documented process for End-User request for active or new service for Avaya Extension to Cellular	Service Manager
Avaya IP Softphone for Agent Incident Request	Documented process for End-User request to repair trouble with Avaya IP Softphone for agent service	Service Manager
Avaya IP Softphone for Agent IMAR Request	Documented process for End-User request for active or new service for Avaya IP Softphone for agent service	Service Manager

For quality UC support, Contractor's SMEs shall use numerous automated tools. These tools shall enable Contractor to continuously monitor the overall health and performance of voice appliances, assist in rapid restoration through fault isolation, and perform traffic analysis as shown in the table and discussed further below.

Contractor shall deliver complete manufacturer system maintenance coverage on all County Core Voice Services assets. Together, these tools shall provide complete health monitoring and expeditious issue resolution. Avaya Expert Systems and Secure Access Link shall be online and engaged 24x7 to diagnose and attempt to resolve

known system alarms, clear many service affecting issues, and escalate to engineering resources for prompt attention when necessary.

Contractor's UC team shall use Nectar's UCMP and its complete suite of innovative features to provide the County enhanced, integrated network services. Nectar shall provide multivendor management services including application dependency tree visual alerting and vendor knowledge modules, which shall help Contractor's SMEs proactively pinpoint and resolve cross-platform integration issues quickly and restore services to County users. The UCMP shall also include real-time network quality of service reporting using RTCP integration, and shall be able to create simulated traffic injection between designated network segments for analysis. This shall allow the SMEs to monitor and report on all VoIP related traffic transmissions.

The quality of service reporting tool shall provide per-hop statistics and in many cases shall assist in quickly identifying improper packet handling hop points. The Nectar platform shall include statistical resource utilization data gathering and storage that shall enable trending analysis and capacity planning. These capabilities shall be available using an intuitive and customizable dashboard with visual and electronic alerting from sophisticated threshold configurations. The dashboard shall allow Contractor to acknowledge, respond, and correct issues proactively, in many cases before County users know or report an issue.

4.10. Catalog Services

4.10.1. Process and Procedures

- Description of solution to meet the requirements

Solution Summary. The Optional Item Catalog (OIC) shall hold all approved single user applications, standard and nonstandard hardware items, and support only services.

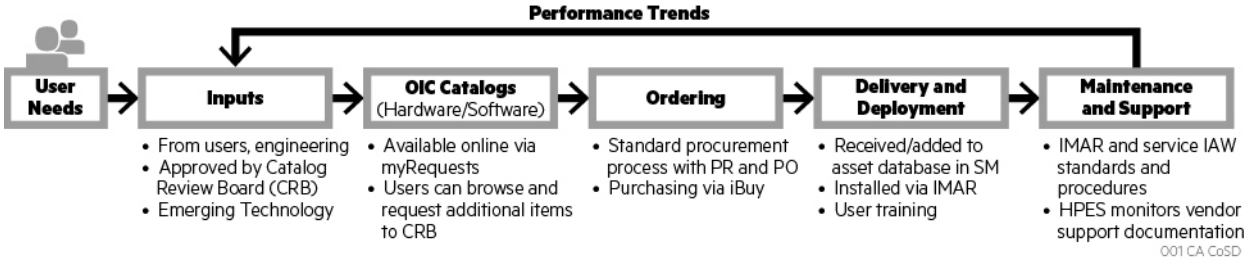
The configuration of the catalog shall be controlled by the Catalog Review Board (CRB). The board shall consist of Contractor and County selected points of contact (POCs) from each department to discuss, review, and approve items for inclusion in or removal from the catalog.

Catalog activities, such as ordering, maintenance, and approval, shall be accessible online via the Service Portal and myRequests. While all users shall be able to order, only select users shall be able to perform other functions––review and approve, for instance—based on their organizational role and authority. myRequests shall be replaced with Service Catalog and Request Manager during the Cross Functional Transition, as described in the Transition Services Framework.

Requirements and requests for new catalog items or updates can come from users, engineering analysis, new technology offerings from HPE, third-party vendors, and elsewhere. County desktop hardware peripherals, laptop accessories, stand-alone printers, and desktop software prices shall be reviewed on a quarterly basis by HPE Global Procurement through a Request for Quote (RFQ). Contractor shall check with suppliers to compare prices and delivery schedules to match the existing catalog and make the necessary changes. Once the catalog manager receives the updated list from HPE Global Procurement, he/she shall update the OIC. The updated list shall be reflected in the following OIC publication, which shall occur on the 20th of every month. The catalog shall be updated with new End-User hardware peripherals and End-User software, including pricing on these items, one for hardware replacement and one for end of life (EOL) hardware.

The figure below provides a summary of the OIC solution—rom identification of item need to delivery and support.

The OIC Process



Once approved, the catalogs shall be available via the Service Portal. Users shall order via myRequests using functionality described in the "MyRequests User Guide."

For nonstandard items that are already installed and deployed, Contractor shall support OIC items through the warranty period for hardware. If additional assistance is needed, Contractor shall implement other processes to provide support for these items.

User training shall be available on OIC items, as necessary. OIC items shall be monitored by Contractor for manufacturer updates and shall be incrementally refreshed as recommended and approved. Specialized End-User support for applications shall depend on the nature of the applications and the problem. Technical and configuration support shall come from Contractor's break/fix technicians. If the issue is determined to be related to an application with a Portfolio Application Identifier (PAID), identifying it as a supported application, Contractor's Service Delivery Manager (SDM) for the business unit shall work with the vendor and the County apps owner for that portfolio application.

Each item in the hardware and software OIC catalogs shall be sorted by category, with a brief description, manufacturer, model/reference, and a unit price. For commercial items, pricing shall be set competitively via Contractor's procurement organization in agreement with the RFP requirements. If an End-User selects an item that requires End-User Service support for installation, those requests shall be added at the end of the optional item ordering process.

On the software side, there shall be three categories of desktop software:

- Purchase - Software products that are available for purchase.
- Supported but no longer available for purchase – Software products that are part of the Desktop Application Directory but are no longer available for purchase (for example, old versions of software). These products are still supported by Contractor.
- Other desktop software - Software that can be installed if licensing is in place. An analyst contacts the requester to discuss licensing before the software is installed.

- Deployment plan for resources and use of facilities

The OIC shall be available via the Service Portal in myRequests, both of which shall reside on servers at the Contractor data center. OIC management and deployment/service of optional items shall involve Contractor resources in management, engineering, procurement, and End-User services, most of whom shall be assigned to the Rancho Bernardo site. Others shall be part of a virtual team from across the U.S.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Online Catalog. The OIC shall list items available for purchase by County users and shall contain standard items as well as optional items. Users shall be able to shop for items available for one-time purchase or RUs (monthly fee), including bundled services. Users shall also be able to suggest changes to the catalog. When an item is

approved and an order is placed, Contractor shall fill the order and deliver the products to the requester. Contractor shall:

- Coordinate an installation appointment with requestor
- Assist with set-up, including physical installation and connection of the device to the workstation or network
- Assist with the initial loading of the software products listed in the catalog,

The OIC is accessed from the myRequests page, which shall reside as a link from the Service Portal.

Viewing/Modifying Catalog Requests

All catalog requests shall be viewable by the requestor but shall only be able to be modified prior to submission. If a change is needed after submission, the End-User shall need to clone the request, make the changes, and delete the old request. The End-User shall be able to see the purchased status of an item by clicking the Purchasing tab.

Reviewing and Authorizing Catalog requests. If an End-User is a reviewer for the Catalog, they shall be able to access requests that have been submitted. These requests shall appear on the Review Catalog Requests screen. After accessing a request, the reviewer shall make comments that are then sent back to the requestor, rejecting or approving the request as submitted.

Shopping from the Catalog

An End-User shall be able to order hardware, software, or services from the catalog including video conferencing equipment, audio-video equipment, and telephones, computer and phone services, or special bundles for new employees. For all catalog orders that involve site installations, they must be authorized by the County Technology Office, who shall be notified by the myRequests system.

Billing, Authorizer, and POETA

After a request is made, the End-User shall be prompted to enter their billing and authorization information. myRequests shall use this information to "file" the request with the appropriate County agency and provide the correct financial account management. Each letter in the word "POETA" stands for a different billing item. The End-User can contact the financial coordinator of the business group for the correct information to submit. Billing shall be in accordance with the supplied POETA information.

Procedures. Catalog updates shall be managed in coordination with other standards governance activities, including the annual standard desktop configuration update and the weekly architecture review meeting. The catalog shall be updated in synch with other configuration changes.

The key to continual improvement in the Catalog Services component shall be to perform benchmarking with vendors, making sure that the catalog is refreshed regularly, is responsive to End-User needs, and that catalog optional items integrate and interoperate well with the standardized core configurations. Each new component shall be SIT and UAT tested and approved by the County.

4.11. Network Printer Services

4.11.1. Process and Procedures

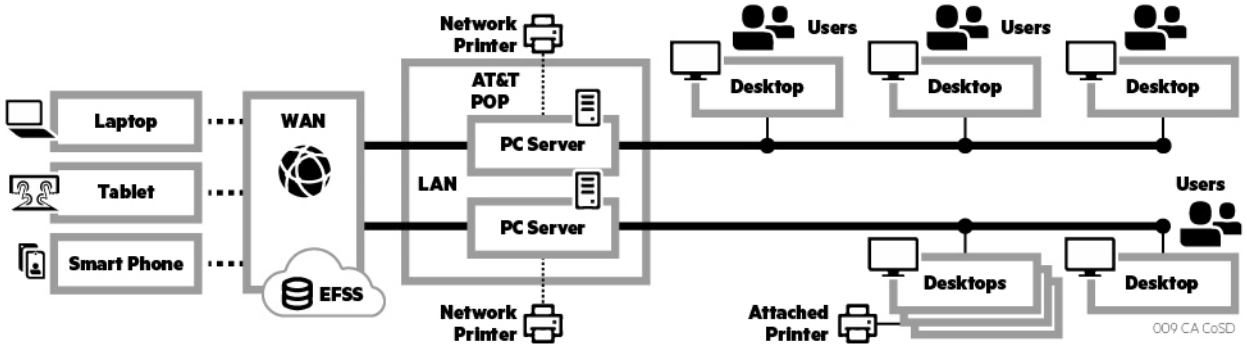
- Description of solution to meet the requirements

Network printers shall be integrated into the End-User service model and network architecture seamlessly.

The network printer support solution shall be the same for all types of printers. The only difference shall be in configuration and utilization information related to specific makes and models of printers. The figure below summarizes the network printer configuration.

Network printers shall be standardized attached devices and are operated and maintained under many of the same procedures for hardware and core software. Desktop services shall handle the printers, their configurations, drivers, and the queues. The local server team shall manage the print servers located in the AT&T POP and in the DR POP location in San Diego, as well as other locations where servers are installed throughout the County (such as FRCs and CAC).

Network Printer Architecture



- Deployment plan for resources and use of facilities

Contractor shall perform this work from Contractor's Rancho Bernardo site.

All service technicians shall have basic training and skills in network printer operations, maintenance, and troubleshooting. Contractor shall have a hardware team that specializes in printer/server support, but all field technicians shall be trained at a basic level to support these devices. Printer specialists shall be embedded in the Desktop Services organization but shall not be a separate team.

Contractor's technicians shall have the same core skills but different levels of expertise in specialized areas, such as surge and DR situations. Because of this, Contractor shall be able to cross-assign staff to a critical area.

- Key methodologies and processes in solution including year-to-year continuous improvement

Printers are a specialized device on the network, but the overall processes and procedures described previously in the End-User framework shall apply to printers. Printer management shall involve printer specific activities such as:

- Printer service IMAR and operations
- Printer device management
- Queue setup
- Load balancing
- Printer security management
- Configuration setup and management for groups and individual users.

The requirements to support network printers shall be part of Contractor's plan, build, operate approach. The table below maps each of the framework component requirements into a Plan, Build, and Operate (PBO) phase and then summarizes Contractor's solution and methodology and key processes.

Mapping of Framework Component Requirements for PBO Phase

STAGE	COMPONENT REQUIREMENT (SUMMARY)	CONTRACTOR'S SOLUTION, METHODOLOGY, AND KEY PROCESSES
Plan	Standardize	• Printers are included in annual engineering and standardization reviews • The County approves standard printers
Plan, Build, Operate	Provide back-end infrastructure	• Printers must be compatible with the County Architecture • Network capacity is engineered to support printers
Plan, Build, Operate	Upon device failure or network failure build in redundancy and failover procedures	• Engineer and maintain for reliability and recovery
Operate	Keep drivers current; maintain firmware (slightly specialized)	• Drivers are maintained via SCCM • Firmware versions are monitored via vendor FAQs and pushes
Plan, Build, Operate	Categorize printers; printers are either standard resource units or in the OIC	• Several classes (monochrome, color, high performance, large format, label and multifunction devices) of network printers are installed • Printers are in Report 44 and the OIC
Build and Operate	Support the User – develop training, tip sheets, update the portal, among others	• User support materials are built by engineering once the printer is selected
Build and Operate	Continuously maintain Service Desk scripts and support info for technicians	• Printer install and End-User support materials are built by engineering • Tickets feedback inputs to improvements
Plan, Build, Operate	Leverage existing licenses	• Printer timeline and refresh strategy is maintained to reduce cost of licenses • Strategic negotiation and leverage utilized for license costs
Plan	Make effective standards at the start of each new year	• Printer standards are selected as part of the annual standardization process • Printer vendors brief County and Contractor on current products and migration path(s)
Plan and Operate	Supply via the portal a list of consumables	• Consumables list to refreshed annually along with the standards selections • The County can therefore forecast consumables expense and do supply management
Operate	Excluded printers not attached	• Concur
Operate	County shall be responsible for consumables	• Concur

STAGE	COMPONENT REQUIREMENT (SUMMARY)	CONTRACTOR'S SOLUTION, METHODOLOGY, AND KEY PROCESSES
Operate	Maintenance, availability, and break-fix	• In agreement with overall service and break/fix methods • Printer experts are available to assist at all Tiers of support
Plan	Maintain and update annually a timeline/roadmap regarding support to active devices and planned tech refresh	• Printers are part of the overall standards assessment, engineering, test and governance The County approves the standard printers and any OIC printers

4.12. [Reserved]

5. NETWORK SERVICES

5.1.1. Process and Procedures

Bandwidth and capacity management and reporting.

Contractor has tailored its bandwidth and capacity management processes to meet the County's increasing needs. Bandwidth shall be proactively delivered to County locations before link saturation affects performance. This process shall begin with weekly reporting on key capacity metrics using AT&T's CA spectrum and eHealth tools. These tools trend bandwidth and latency against baselines. These trends shall be validated as legitimate business traffic using AT&T's deep packet analysis tools before action is taken. Using the thresholds below, which may be modified by mutual agreement of the parties, Contractor's Capacity and Performance Monitoring team shall make recommendations for bandwidth upgrade in the weekly Operations Governance. This approach to capacity management helps the County of San Diego provide the right level of capacity at the right location and at the right time.

Below are the thresholds for both WAN and Internet Transport:

Bandwidth Utilization Threshold (WAN): 90% Peak Utilization over 4-week period of time + corresponding latency threshold breach
Bandwidth Utilization Threshold (ISP): 90% Peak Utilization over 4-week period of time + a 1.5 – 2Mbps drop rate
Latency (WAN): GigaMAN (greater than 4ms), Opt-E-MAN/NoD (greater than 8 ms), T1 (greater than 15 ms)

As part of this process, Contractor shall provide:

- Weekly review of network capacity metrics as part of the County's operational governance process.
- Capacity management that meets the business needs of the County using tools that provide real-time threshold alarming.
- Communication of findings and recommendations that help the County achieve optimal utilization and capacity.

The local team shall continue to meet weekly with the County's operational team to present and review findings and make recommendations. Contractor shall perform optimization analysis daily using its automated tools that aggregate findings and establish trends that become the basis of Contractor's weekly reporting.

Contractor shall migrate remote sites to AT&T's Switched Ethernet (ASE) with Network on Demand. This allows the bandwidth and capacity management practices for the County to become even more dynamic. Using the software-defined networking capabilities that are inherent to ASE with/Network on Demand, bandwidth can be adjusted from as low as 2 Mbps to as high as 1 Gbps in 15 minutes.

Contractor shall implement a solution whereby adjustments can be made within the Network on Demand infrastructure on a scheduled basis, providing the County a great deal of flexibility in bandwidth management. As an example, if the County Health and Human Services Agency planned an employee training event that required heavy video and interactive content (not distributed using a centralized, multicast town hall solution), Contractor's capacity team schedules an adjustment to specified remote sites for an agreed period of time. This shall deliver the required bandwidth where needed and, at the completion of the training, automatically adjust the bandwidth back to its normal business capacity.

Real-time bandwidth adjustments shall also be made as needed. This may be required as the result of unexpected local or national events creating unanticipated demand on the data network. As future events occur, Contractor shall be able to do more than just increase the ISP bandwidth. By using its capacity and performance monitoring

tools, Contractor shall analyze the traffic and determine if it is affecting the County's WAN. At that point, real-time adjustments shall be made to alleviate the congestion in minutes.

All transport services—including WAN, AVPN/MPLS, ISP, and SIP trunking shall be scaled to maximum interface capacity as well as built in parallel so that growing County bandwidth needs are met over the life of the term. Also, as new services are made available with additional speed or throughput capabilities, Contractor shall require AT&T to evaluate the feasibility of such services and make corresponding upgrades where reasonable under existing service commitments.

Performance monitoring and reporting

Contractor shall provide the data necessary to optimize network service to the County. Capacity planning is used to determine the network resources necessary to prevent performance issues from impacting these critical network services. Performance monitoring/management is the process of managing network and data services response times, consistency, and overall service quality.

Contractor's network team shall administer, monitor, maintain, and manage performance of the data network services and network services infrastructure. This shall involve input from many areas of the business to identify what IT infrastructure is required to support the County's business.

The process components shall include:

- Performance monitoring for routers, switches, firewalls, and network servers and appliances
- Capacity monitoring of WAN transport circuits
- Internet performance monitoring of public and staff CIR
- Trend reporting and analysis.

Key sub-processes shall be:

- Network bandwidth monitoring to specified thresholds
- CPU/memory utilization and errors monitoring on all network devices to specified thresholds
- Responsive impact assessment and mitigation planning
- Proactive trend-based "situational watch list" assessments and corresponding action plans
- Real-time traffic analysis initiated from "exceeded threshold criteria" in the form of Spectrum critical alarms.

Performance Monitoring Tools

Using AT&T's capacity and performance management functions that utilize various toolsets, Contractor shall provide monitoring, reporting, trending, and analysis services to the County.

CA's eHealth and Spectrum tools shall integrate to maintain critical service levels across complex network environments by combining eHealth's automated availability and performance management with the Spectrum network service and analysis platform.

The eHealth and Spectrum tools shall allow for more efficient alarming and reporting, enabling the network capacity and performance management team to focus on proactive troubleshooting, performance optimization, and service level management.

Another toolset that shall help manage system performance within the County network infrastructure is Riverbed Cascade Profiler, which provides a unified end-to-end view of service delivery, application, and consumption from the data center to the End-User. Cascade Profiler assists in troubleshooting the threshold deviations reported in eHealth, troubleshooting in real-time and from a single probe interface. Cascade retrieves real-time

information, providing quick and easy access to logical views such as link analysis, link usage over time, Top N applications, and Top N conversations and hosts.

Troubleshooting and Forensics

The above mentioned promiscuous tools enable event correlation and forensics through the active capture of network traffic combined with reporting capabilities that provide real time and historical data. This capability applies not only to the previously mentioned tools, but also includes the deployment of desktop based tools such as Wireshark, which are used as needed to conduct packet captures from individual assets. When used in active troubleshooting, all of these tools are used to correlate the event to a root cause for resolution by the appropriate framework using cross framework troubleshooting processes.

Performance Baselines

Contractor shall use these tools to provide data on specific metrics for historical and baseline performance evaluation. These baselines are important in Contractor's monitoring of the County's network since they can directly affect bandwidth provisioning and other resources.

Performance Threshold Alarming

Once baselines have been determined, thresholds shall then be established based on variables within the network infrastructure. Circuit measurements depend on bandwidth to determine baselines and thresholds. Physical devices such as routers and switches report memory allocation errors, CPU utilization, and buffer hits. There are also broader ranges of environmental specifications to which thresholds are tracked, such as power supply, fans, and temperature, among others.

Threshold severity is currently defined in four levels, each dictating an appropriate course of action as listed in the table below.

Threshold Severity

SEVERITY	ACTION
Warning	Track element status on weekly basis.
Minor	Add to Watch List (document in Situation-to-Watch and status any changes).
Major	Assess and engage relevant framework, open internal ticket if necessary. Add to Watch List.
Critical	Trigger to "Attention" notification tool, initiate internal break-fix. Troubleshoot and actively mitigate until resolution.

Critical alarms shall be sent to the Attention application system that notifies the NOC operations team (and on-call) members via phone, SMS, and email. The Attention system software shall provide a predefined notification process for critical alarms as well as escalation processes for overdue or pending alarms on a 24x7 basis.

Other important thresholds that have been established include site latency and Internet CIR thresholds. Site latency thresholds shall include latency deviation based on the type of circuit. Internet CIR thresholds shall be triggered when bandwidth use on the Internet link goes 20% above the daily average, as measured by eHealth and in conjunction with quality of service (QoS) policies applied to the Internet router.

Performance Trending and Analysis

Once baselines and thresholds have been established, Contractor shall perform trending and analysis. There are a number of variables that contribute to the analysis of a trending element. Bandwidth use, CPU use, physical

hardware errors and application response time delays can all have an impact on network health. eHealth reporting (Situations-to-Watch, Top N Reports defining baseline statistics, Health Index Reports indicating CPU, errors, and discards) along with Cascade Profiler reporting (application response time statistics, link usage, top application layer applications and hosts) shall be used to collectively qualify and pinpoint performance degradation associated with the network or an application. This detailed information shall drive necessary corrective actions as well as engagement of the appropriate Contractor framework in problem resolution.

Reports showing an increase in trending for elements in the network shall be reviewed and investigated for further analysis. Report trending from Situations-to-Watch, Top N latency, and health index reports shall be addressed by further analysis with a deeper dive into the affected element(s).

Adjustments made to correct issues associated with variables related to bandwidth use, memory allocation errors, CPU processors, or other changes in the network, shall be based on investigation of the specific cause. Increasing the bandwidth for a specific County site shall be determined by identifying historical data and trending analysis for a specified period of time. There shall be an initial assessment and continued monitoring of the network thresholds (application, End-User count, throughput and other associated activities) to validate the appropriate remedy for a given issue.

Real-Time Anomaly Detection

As the Contractor Operations team begins developing processes around real-time anomaly detection, they shall develop automated alarming and event correlation capabilities, with focus on application performance. The tools mentioned in this section—along with other data center and desktop-based platforms—shall enable a layered approach to event triangulation, which, combined with the daily stand-ups, improves the proactive performance management of services across the enterprise. Contractor shall dedicate resources to improving proactivity over the life of the term, with measured results reported through the operations governance process.

Data Aggregation and Analytics

Contractor shall contribute key capacity and performance tool data to the cross functional data warehouse, with focus on bringing enabling automation and continuous improvement through a global analytics and reporting practice.

Contractor shall work with the County in extending both the data contained in the data warehouse as well as the BI/Analytics platform to support a more complete IT Service Management Analytics capability. The benefit to the County can be measured as follows:

- Service Strategy and Improvement Analytics: This area focuses on analysis that supports recommendations to improve business outcomes and improve customer satisfaction. Analysis of available data sources can be used to assess; IT Infrastructure Health, IT Transformation alternatives, predictive analysis of customer satisfaction, and customer sentiment analysis

- Service Design Analytics: This is a way to use analysis to better understand capacity demands and service availability by predicting degradations, preventing outages and reducing downtime. Using ITSM data Contractor can forecast demand and utilization on the infrastructure, predict service degradation with the goal of reducing system downtime.

- Service Operations Analytics: Blending ITSM data and benchmark IT performance data, Contractor can conduct analysis to reduce business impact of events, incidents, and problems.

- Service Transition Analytics: These analytics address the correlation of incidents and events to root causes in order to speed recovery and to identify ways to reduce IT complexities.

Performance Reporting

Contractor shall ensure that tools are in place, baselines and thresholds are completed, and trending and analysis processes are established to provide reports to the County that affect not only bandwidth provisioning, but adjustment and potential corrective action to a wide variety of County resources. On-demand reporting shall be available upon County's request for fast turnaround on critical and time sensitive issues.

Trend and health reports shall be scheduled monthly to collect data and identify the top volume and health index leaders throughout the County network infrastructure. The report shall identify contributors that qualify for threshold conditions such as, use, CPU, memory, errors and latency.

Elements each month shall be sorted by the Top N elements and performance indicators that require attention or resolution. A summary analysis shall be presented for the monthly activity and shall provide watchful situations or those exceeding threshold limits that require corrective actions.

Included in the monthly reports shall be a "Monthly Summarization Report." The details in this document shall include opened tickets for County sites that were affected by latency, bandwidth, errors, CPU, and memory related performance issues.

New and layered approaches to integrating capacity and performance and real-time anomaly detection shall be defined that leverages multiple toolsets. This shall involve cross-framework teams that proactively respond to enterprise issues affecting End-Users.

Identification and Elimination of single point failures in Network Services.

The County increasingly relies on the continuity of the data network for its business functions to remain operational under any circumstance. With this in mind, Contractor shall focus heavily on redundancy and survivability of critical core network services.

Contractor shall avoid single points of failure in its network elements (such as circuits, central offices, and core network elements) via AT&T's redundant network design and software defined infrastructure. These redundancy solutions allow Contractor and AT&T to maintain continuity of the regional, nationwide, and global backbone in the event of isolated failure. One dynamic of the County network solution leverages this redundancy through the use of diverse pathway and ISP exchanges in both San Diego and Gardena, California. With this configuration, the geo-redundant County ISP service remains dynamically available in the event of a regional service interruption.

Increase of visibility into all data communications and data flows between End-Users and Services within the Data Center.

Effective tools are not the problem facing proactive performance management. It is the practice of modeling, trending and analysis that can unlock the potential of the data the tools can deliver, if performed with a broad understanding of the enterprise.

Contractor shall create a cross-framework predictive analytics team whose charter is to manage performance on an enterprise basis. This team shall create and execute a repeatable process to be documented in the Standards and Procedures Manual using a layered approach using numerous tools to monitor and respond to shifts in baseline data.

By developing baseline traffic patterns for network, application, desktop, server, and management traffic, this team shall define thresholds and event patterns, allowing the team to take predictive action, correlating anomalies in the environment. Using the multiple sources of data, Contractor shall conduct daily stand-up calls where threshold breaches are evaluated and diagnosed. This team shall open internal operational tickets on the issues and shall have the authority to escalate across any framework to engage resources as needed to respond and identify

the source of the anomaly. Ongoing reports shall be provided to the County operations team and covered in weekly governance meetings, identifying open issues that are being monitored as well as successful closures.

Contractor's County Operation team shall also be tasked on an ongoing basis with improving processes, tuning their practices to better predict, correlate and resolve anomalies. This team shall also have the responsibility to train on their tool sets, improving their mastery in the art of performance analytics. Further, Contractor shall evaluate new and emerging tools that it proposes for implementation, adding to the depth of the data sources at the County's disposal.

The members of this team shall be identified by each framework as responsible for performance management in their discipline and will dedicate the necessary time to maintain a best in class performance analytics function. By taking early action, this team shall drive through chronic issues and eventually reduce the effort for their resolution. Tools and practices, effectively used together, shall increase the visibility of anomalies across the enterprise, improving the End-User experience while maximizing organizational performance and business output.

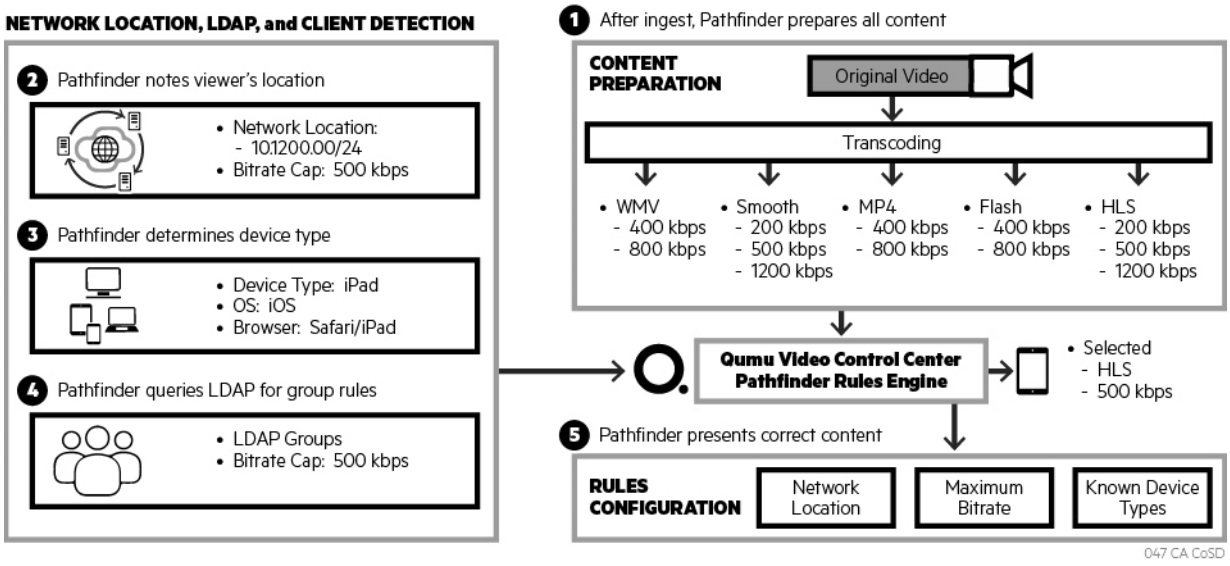
Town Hall Services.

Contractor shall use AT&T Video Management Services (AVMS) and its partner Qumu to provide town hall video services for the County.

Through AVMS, Contractor shall provide all of the functionality needed to capture, manage, and publish video content for both live and video on-demand (VoD) distribution for local and remote users. AVMS's advanced transcoding capabilities shall support formats from various capture devices—from production studio and video conferencing platforms to mobile devices and video cameras. For distribution, the solution shall allow for consumption of video content on a wide variety of devices such as laptops, desktops, tablets, and smartphones while optimizing the End-User experience based on the device being used and bandwidth available.

By means of Pathfinder, AVMS' intelligent routing and distribution element, Contractor shall optimize and present content viewing based on device, network location, and bandwidth, as illustrated in the following figure.

Optimization of Content Viewing



Contractor shall use subdomains to provide separate access to video intended solely for users on the County domain, such as internal communications or training. Internal and mobile video viewing shall have the option to be limited to specific groups based on active directory (AD) group.

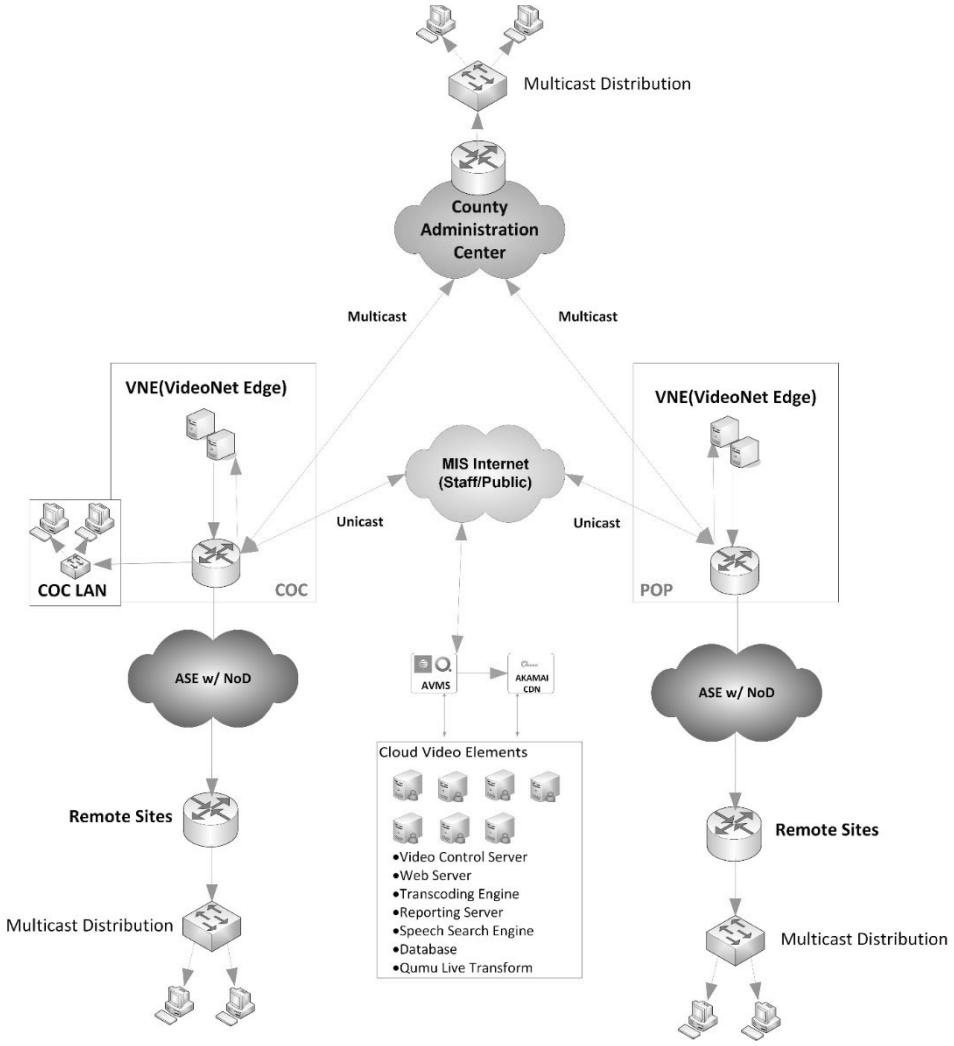
Embedded polling and feedback features shall be included to offer increased benefit to the County by engaging viewers and soliciting their input. Contractor shall use high grade analytics to provide viewer statistics along with broadcast performance detail to provide a clear picture of content performance and identification of possible impacts.

AVMS offers both on-premises and cloud-based options. Contractor shall use the cloud-based architecture, which provides high availability without the need for extensive local hardware and associated support costs. With the added benefit of burst capacity for mobile or public users in real-time, the solution is able to handle traffic spikes without degradation of the delivery quality. The hosted solution can scale to cover all of the County users with growth up to 100,000 simultaneous viewers. With archiving capabilities, video content can be preserved and made available for replay for a configurable length of time.

AVMS makes use of both internal and external Content Delivery Network (CDN) technology. For external content delivery, Contractor shall leverage the Akamai platform. This external content delivery shall be used to augment or replace the Granicus streaming solution.

From within the County domain, the AVMS solution shall enable multicast video presentation through VNE's (VideoNet edge) to multiple viewers simultaneously without causing an exponential impact to network performance. Contractor shall implement four VNEs, two at COC and two at POP. From this geo-redundant core, the multicast stream can be routed across the WAN to the remote edge, where the LAN redistributes the stream to each requesting End-User.

AVMS Topology



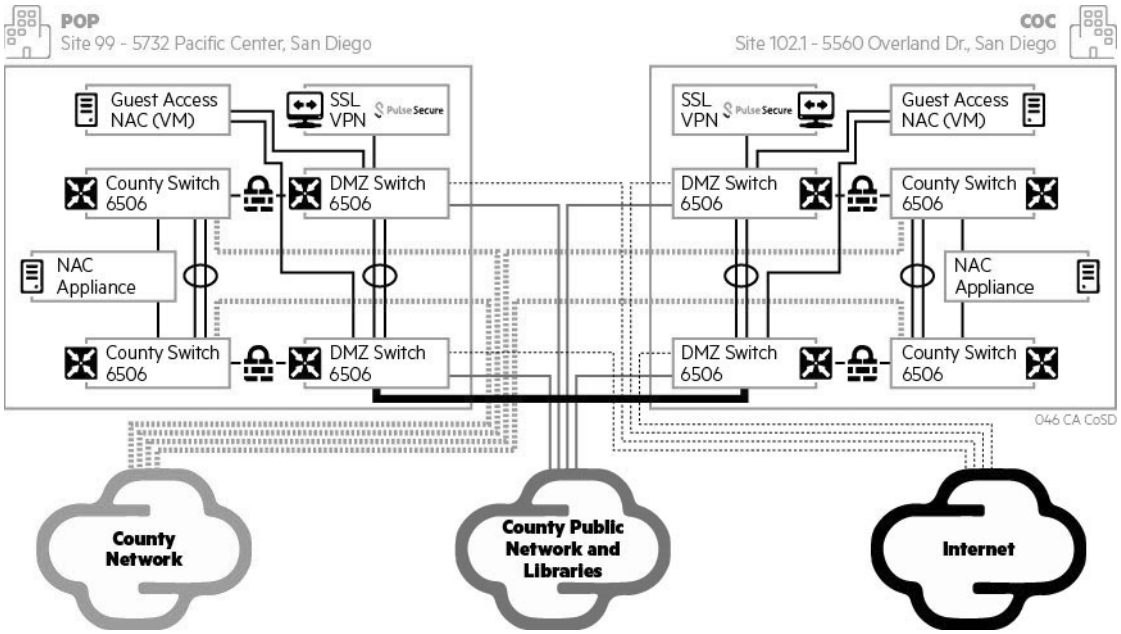
Topology of the AVMS solution, highlighting cloud based services feeding geo-redundant Video Network Edge devices that feed multicast video streams to the remote County sites.

In order to represent a complete solution with no limitations to the County, Contractor is only Providing AVMS for enterprise video content distribution. Contractor shall implement this service within one year of County approval. The solution shall be charged through a fixed monthly Resource Unit Fee for an unlimited number of townhall events. Such RU Fee may be allocated to business units based upon the County's discretion.

Network access controls and PKI-based device authentication for Wireless Services.

Contractor shall use Aruba's Clear Pass Policy Manager (CPPM) to provide a comprehensive yet integrated NAC solution. This product shall provide the County all the features of NAC in a single platform to ease management, administration, and troubleshooting efforts. Contractor shall use an integrated RADIUS server, coupled with the ability to perform guest access authentication, shall provide a wireless solution enabling County staff and the public appropriate, policy based network access across any access point in the County. This solution shall provide a seamless authentication for the staff while allowing various options for the redirection of public or untrusted devices. While the wireless deployment is planned to be implemented first, the solution shall function on all physical ports Countywide.

NAC/Guest Access



NAC/Guest Access centralized management topology is provided via a geo-redundant architecture.

The Aruba NAC solution shall be implemented to align with Contractor's geo-redundant, high availability standard. One appliance shall be located at the AT&T POP and one installed at the County Operations Center (COC). These appliances shall manage and enforce policy on the staff wired and wireless infrastructure by leveraging 802.1X and EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).

The solution shall allow any County domain joined device that is plugged into the network, and logged into with a valid active directory account, to be given access to County network resources. Any devices plugged into the wired network that do not meet the above criteria, or predefined NAC policies for non-domain joined or non-dot1x compliant devices, shall be placed onto a public VLAN with restrictions that allow for access to the Internet only.

The integration with the existing wireless infrastructure shall continue to leverage EAP-TLS to validate certificates for access to the existing County secure wireless network. The certificate required to authenticate, as well as the wireless profile, shall be installed at the time a computing device is prepared for distribution by means of a group policy object (GPO) push within the desktop framework. This GPO is the only way the client machines can receive the certificate required.

To provide public guest access, the Contractor shall install a virtual instance of a clear pass policy manager in the DMZ at both the AT&T POP and the COC for redundancy and resiliency. This provides guest access on the public Wired/Wi-Fi network. The solution shall force all users of the public network to view the captive portal splash page where terms and conditions can be presented and must be accepted prior to being granted access to the Internet. The contents of the splash page, as well as the look and feel (theme), can be modified to include desired content or photos and provide automatic forwarding, after acceptance of terms and conditions, to the County's home page.

The guest access solution shall also offer functionality that shall be leveraged for business unit specific use cases.

Contractor shall maintain a RADIUS server (steel belted radius [SBR]) that acts to authenticate radius sessions from the wireless network. The Contractor team shall leverage the two Aruba appliances planned to be installed at the AT&T POP and the COC to provide radius server functionality in place of the existing SBR server. The two

appliances shall be fully redundant, thereby removing a single point of failure and providing all services currently offered by SBR. Contractor shall integrate the new radius servers with the Microsoft CA infrastructure, as well as the new Symantec-managed PKI solution.

Generally, staff users are unaware of any additional security when using a managed County computing asset. The EAP (Extensible Authentication Protocol) required to validate the End-User and machine shall leverage currently logged-in End-User credentials and domain membership to allow access.

Transformation Opportunities

Currently, the County is evaluating cloud-based services to provide cost-effective ways of delivering services to employees and constituents. Contractor's team has already identified the transformations required to receive the full benefits of cloud architecture. Contractor is proposing an AT&T NetBond solution that extends connectivity using a Multiprotocol Label Switching (MPLS) network into County-selected third-party vendors. The NetBond solution provides a secure, performance-assured interface to the cloud, while offloading the Internet Service Providers (ISPs) and dedicating bandwidth to the services. Additionally, Contractor's proposed solution facilitates fully integrated and centralized connection management functionality and supports third-party cloud services with Contractor's contractual service levels.

The foundation of this service is to be deployed in a geo-redundant manner, using AT&T Virtual Private Network (AVPN) MPLS circuits; it is included in the Data Network Services and is priced. Future implementations of NetBond services (proposed as a resource unit (RU) on a bandwidth basis) use this transport connectivity to create the peer-to-peer connection with the selected cloud provider (cloud provider costs may apply).

In support of the transition of Exchange to the O365 cloud, and in line with Microsoft's recommendation, Contractor shall ensure adequate bandwidth is provisioned on the geo-redundant Internet ISP's to allow access to O365 services. As an option for isolating this service away from the ISP, Contractor shall also offer optional NetBond functionality in a peering arrangement with Microsoft's Azure Express Route product. The solution shall be evaluated as a part of the design effort and shall be offered as an optional service, and priced as a separate RU that combines the NetBond RU with the Express Route costs to complete the connectivity model for the service.

5.5. Data Network Services

5.5.1. Process and Procedures

Collaborative Approach

Through involvement in weekly CTO architecture sessions, as well as participation with the Enterprise Architecture (EA) governance process, Contractor shall propose new technologies that have been evaluated and measured against County strategy and business requirements. This continual dialogue with the County, along with Contractor's broad industry knowledge of network solutions and their impact on adjacent technical disciplines, allows the Contractor team to successfully propose and implement emerging technologies within or even before the agreed-upon technology refresh cycles. This approach allows the County to quickly realize the benefits of new technologies. This ongoing interaction also facilitates the standardization of hardware and software deployed by the Contractor team as its solutions receive initial approval from the Enterprise Architecture Forum and subsequently from the Change Review Control Board prior to transformation.

Upon activation of its approved solutions, Contractor shall employ several automated tools to maintain an accurate and up-to-date inventory of all hardware and software supporting data network services. In addition,

Contractor shall use automated tools to continuously monitor the provisioned services from an operational and bandwidth utilization perspective, as well as provide valuable insights into traffic patterns and application functionality.

Monitoring and Management Approach

From an operational view, Contractor's capacity and performance management tools shall continuously measure and report on delay, packet loss, retransmissions, bandwidth use, and service interruptions. In the case of an outage or degraded services defined by specific thresholds, automated alerts and page-outs shall be sent to Contractor's local, dedicated team members who respond to resolve incidents within Service Level Agreement (SLA)-specified parameters. During normal business hours (6 a.m. – 6 p.m.), the engineering and Service Desk teams shall monitor operational status using CA Spectrum and actively respond to alerts. After hours, the Contractor team shall use the automated notification features within the tool to provide the necessary alerts that trigger incident response activities within stipulated SLA parameters (24x7x365).

As part of Contractor's prompt restoration services, Contractor shall report incident response activities to the County using the centralized Contractor Ticketing System. Additionally, on P1 and P2 outages, as well as upon County request, Contractor shall develop root cause analysis documentation and submit it for review. Incident reporting also includes a proactive response to performance or capacity issues, and Contractor's reporting shall clearly identify the nature of the incident or degraded performance and the steps taken to resolve the issue.

Contractor's network performance management shall also use CA Spectrum to provide monitoring. One component of CA Spectrum is CA eHealth, which Contractor shall use to perform trend analysis based on historical measurements as well as current indicators to model, optimize, plan, and report on network services. This tool allows Contractor to meet the County's requirements for speed, reliability, capacity, and quality. CA eHealth also provides real-time and predictive performance analysis capabilities, enabling identification and provisioning of increased bandwidth capacity prior to reaching End-User performance issues on the intranet or Internet.

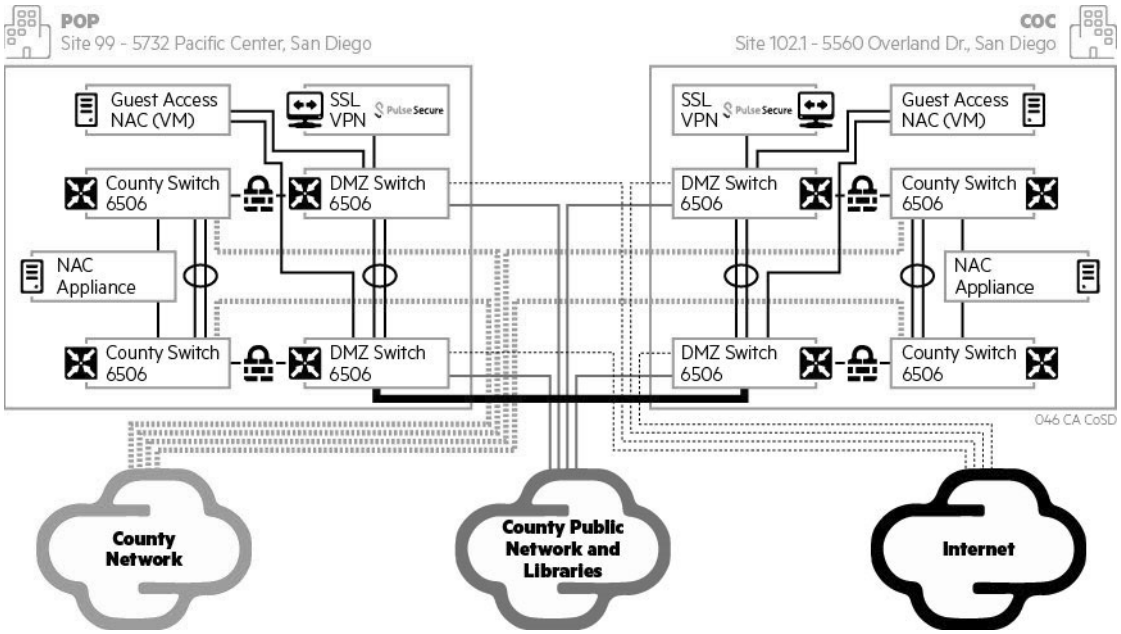
Although CA Spectrum provides passive network monitoring and measurement techniques, Cascade Pilot and Cascade Shark allow active capture, measurement, and analysis of network and application traffic in support of anomaly detection and forensics. The Contractor team shall use these deep packet analysis tools to trend application network performance—establishing thresholds that can be alarmed, correlated, and compared to baselines, enabling a proactive approach to identifying application or desktop issues. Additional network-based tools shall be used to enable a layered approach to trend analysis and event correlation, including Security-based tools such as Palo Alto's Panorama (packet capture and analysis, application identification, traffic volume identification, malware detection, and threat identification); Wireless tools such as Aruba's Airwave (Wireless capacity/ performance); and Voice tools such as Nectar (quality of service [QoS], mean opinion score [MOS], jitter/latency measurement, and round-trip time [RTT] analysis). As Contractor continues to evolve its approach to real-time anomaly detection, new tools and processes shall be evaluated and proposed—improving Contractor's capability to support adjacent frameworks in identifying enterprise anomalies.

Continuous Improvement

Contractor's network shall provide maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest security and service levels. Acting as an "enabler to the enterprise," Contractor's network shall allow any device—managed or unmanaged—to be evaluated, authenticated, and allowed policy-based access. This next generation network shall transform the enterprise by reducing cost and increasing flexibility while improving security and service levels. This new technology shall be expanded in the new term, replacing Opt-E-MAN circuits as well as T1 circuits where possible.

The following figure shows the future state of the centralized, geo-redundant, high-availability network core.

County Network – Future State



County network transformation (future state topology) takes advantage of AT&T's latest software defined network and cloud-based solutions, simplifying the network topology while improving performance, availability, and security.

- Deployment plan for resources and use of facilities

The Contractor network framework team shall maintain infrastructure in County facilities and work closely with the County Technology Office and the Department of General Services to support accessibility and security.

The local life cycle management (LCM) team shall consist of dedicated, full-time resources—many of whom have worked on the County's network for a decade or more. The Contractor network team's primary location shall continue to be in San Diego. All LCM technical, operations, and project management personnel work out of this location. All network services framework components shall rely on the use of the AT&T point of presence (POP) and the County Operations Center (COC). These two geo-redundant sites shall be the core locations holding the centralized communications equipment, appliances, and transport capabilities that securely enable feature-rich capabilities to every business area within the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

The Contractor team shall apply the following key methodologies in its solution:

- Iterative and bi-modal approaches to solution evaluation: "Start fast," evaluate options, and align solutions to County business needs and long-term strategies; establish proofs of concept, all prior to discussion on cost/price.
- Weekly architecture team collaboration sessions allow a continual transformative approach to be maintained across the entire network framework.
- Weekly Enterprise Architecture Reviews enable cross-framework dialog so that adjacent requirements are understood and delivered.
- Contractor employs ongoing, discipline-specific technical roadmap development.
- Contractor uses a structured refresh process, at 4 years, for core routing infrastructure; and 5 years for LAN switching infrastructure. This approach shall be continually reviewed with the County, making certain that the

refresh activities bring the greatest value to the County, with options for deferral provided while taking service level performance into account.

5.6. Remote Access Services

5.6.1. Process and Procedures

Contractor shall maintain its scalable and secure remote access solution to provide the necessary breadth and depth of functionality. In close coordination with the County, Contractor shall maintain a suite of remote access services via Secure Socket Layer (SSL) connections to satisfy the County's evolving requirements through numerous transformation initiatives.

Contractor's experienced, on-site dedicated staff members shall maintain safe, reliable, and secure sessions allowing End-User-role appropriate access to County resources as dictated by County policies and enforced through the use of groups established within Active Directory (AD). This solution set offers an inherent advantage by leveraging the existing AD capabilities. This solution precludes the need to logically connect a disparate system to AD.

To maintain the security and privacy of County resources, Contractor shall establish specific Active Directory group profiles that allow users and capabilities to be directly tied together through specific rule sets for each End-User within the group. Thereafter, Computer Services Registration Form (CSRF) tickets shall provide the direction and authorization needed to assign specific users into their designated profiles. As a result of their specific group membership, users shall be allowed access to a predefined set of resources and precluded from accessing other resources. In this manner, Contractor staff shall enforce County-directed policies.

The Contractor remote access services shall be provided via two independent resource units, Network Persistent VPN, (Virtual Private Network Level 1) and Application Persistent VPN (Virtual Private Network Level 2). These two resource units may be subscribed to stand-alone or in combination and shall apply to the infrastructure, maintenance and support of the hardware and software behind the remote access technology. Base access costs shall be recovered through the Network Access Wired/Wireless RU and shall apply to all County domain registered users.

PulseSecure SSL VPN – Network Persistent VPN (Virtual Private Network Level 1)

Contractor shall maintain geo-redundant remote access gateways from the County Operations Center and the AT&T POP. This solution shall use PulseSecure PSA7000 appliances in the two POPs in conjunction with PulseSecure software loaded on the laptops to facilitate SSL virtual private network (VPN) access into the County domain. This solution shall work with wired and wireless configurations.

Contractor shall continue to evaluate any changes to the environment to identify potential single point of failures and shall work with the County to eliminate them.

This solution shall have the capacity and flexibility to expand, as needed, to support additional users and profiles beyond the existing 2,600 remote users. This scalable solution shall support three profiles—SSLVPN1_D, SSLVPN1_DRW, and SSLVPN1_DRWF. Network access control shall be achieved through a feature known as host checking; the remote host shall be verified as being either a County-owned device or a non-County device and granted domain access as appropriate. For those with full domain access this solution shall provide further granular control by restricting or allowing the use of additional features.

The PulseSecure client loaded on the County-managed laptops (as well as managed mobile devices once that project, which is currently in flight, is completed) shall allow full network access to any and all resources available to the End-User when connected on the County LAN. This client-based connection shall associate each

session with a unique IP associated only with the specific End-User's SSLVPN connection for the duration of his or her connection. This connection shall be logged as well as tracked and reported as necessary, and it shall be used during troubleshooting activities that can be isolated to each End-User session.

At the End-User's discretion, a web portal connection shall be initiated by browsing to a URL and authenticating via the End-User's AD username and password. From within the browser session, users shall have the option to perform up to three activities based on their membership privileges:

- **Initiate a terminal services session (remote desktop)** back to their own County desktop (if configured) or another County network device configured to accept terminal service connections. From there, users can perform normal LAN activity within that remote desktop session as well as create bookmarks for quicker access in future sessions.
- **Browse to County intranet sites** (such as Insite) using the browse function within the web portal window. Users can create bookmarks for these sites on their main web portal page.
- **Access file shares** that users have been granted permission to access, and create bookmarks to these shares.

All of these actions take place within the web portal window. Anything done outside of that window, including web browsing using a separate window or tab, does not flow to the County network.

There are two remote access security features available for transformational use:

- **Security posture evaluation** assesses a device's security posture by determining the presence, versions, and levels of antivirus, spyware, and malware protection as well as operating system (OS) version and patch level, software patches, and disk encryption.
- **Role-assigned remediation** allows the restricted network access of devices for the sole purpose of performing remediation of any failed checks found during the security posture evaluation.

.

Another feature of the PulseSecure solution is direct support for smartphones and tablets provided by installing the PulseSecure mobile application onto these types of devices. However, due to inherent limitations with these mobile devices at present they cannot be configured to automatically sense the unavailability of one gateway and connect using the alternate.

Currently the PulseSecure mobile client is not "connection aware" and is unable to dynamically reconnect to a secondary gateway in the event the connection to the primary gateway fails. Contractor has initiated feature requests and roadmap discussions with PulseSecure to address the manual failover inherent to the mobile VPN solution for the County, which shall be implemented at no additional cost to the County. If this feature does not become available in the first 9 months of the Agreement term, the Contractor shall evaluate and implement a global load balancing solution such as F5's GTM (Global Traffic Manager) by the end of CY 2 of the Agreement at no additional cost to the County. This solution shall involve the installation of two virtual appliances leveraging Contractor's existing virtual infrastructure at both the POP and COC. This solution also possesses the potential to be leveraged for other services such as Mutare Voicemail to Email Service and could extend the capability of global load balancing to all solutions offered externally from the COC and POP.

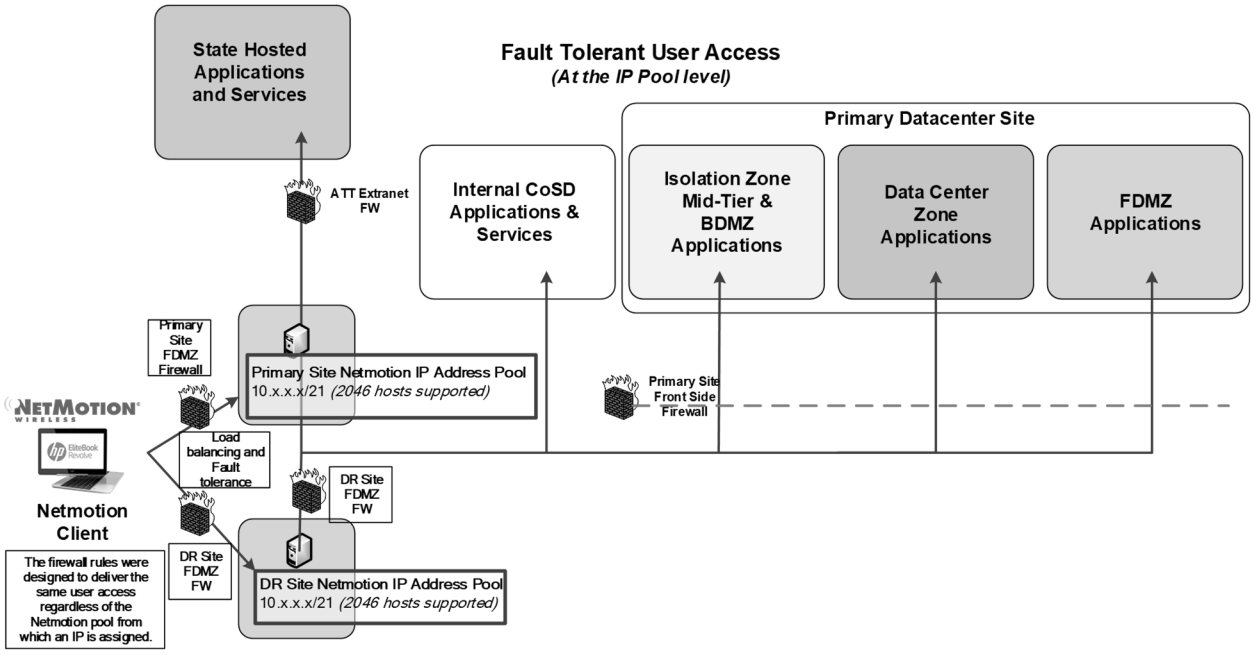
NetMotion – Application Persistence (Virtual Private Network Level 2)

Contractor's remote access solution shall include application-persistent capabilities through its deployment of NetMotion Mobility VPN. Similar to the SSL VPN System, the application-persistent capabilities of NetMotion are enabled by assignment to the correct group profile, which also determines which specific application an End-User may access. Currently, there are approximately 1,200 mobile workers who require VPN connectivity and application persistence to support their business objectives and who require connectivity to the County as they roam between networks. In the new single data center model, NetMotion shall be configured for high availability

with redundant servers load balanced and takes advantage of the built-in redundancy within the data center for storage, network, electrical, etc., as well as the redundant connections to the data center.

Contractor shall deliver an environment that supports mobility session persistence for County mobile workers as they roam wireless carrier networks throughout their business day. Also, it considers the internal County and external County network destinations to which mobility users must connect for successful business productivity. Contractor key objective is to manage the mobile End-User traffic efficiently so that business traffic traverses the links to the applications within the data center and internal County networks, but non-business traffic is redirected through the wireless carrier network or broadband connection. This capability is known as split-tunneling, and it maintains the performance and security of the County's network. A depiction of the logical solution architecture is presented in the following diagram

Figure 2. Fault Tolerant User Access



Remote Access Services

- Deployment plan for resources and use of facilities

For continuity of Contractor's existing geo-redundant network and remote access capabilities, Contractor shall use the AT&T POP in the County as well as the County's Operations Center to hold the Mobile Access Gateways, VPN appliances, and to facilitate circuit terminations. The NetMotion application-persistence solution shall be hosted on highly available and load-balanced virtual machines within the primary Contractor data centers. Contractor shall maintain the NetMotion solution infrastructure in accordance with the standard procedures and policies, while supporting the application with guidance from NetMotion.

Working from its local facility, Contractor's SMEs shall monitor, support, and maintain the remote access services. Any client side issue support shall be initiated through Contractor's Service Desk process.

- Key methodologies and processes in solution including year-to-year continuous improvement

Through the Contractor team's routine involvement within the Enterprise Architecture Forum meetings, the Contractor team's SMEs shall maintain an in-depth understanding of the County's remote access needs and proactively prepare Solution Design Documents for County approval. Thereafter, Contractor's planning and testing of the solution shall allow activations to go smoothly, with back-out plans executed if required.

When a new End-User or group of users requires remote access, Contractor shall gather requirements and determine the type of access needed. For SSL VPN and Application Persistence users, new users shall be placed into an Active Directory group with the appropriate level of access and security. For Mobile Access Gateway users, a Mobile Device Management (MDM) solution shall provide the appropriate level of access and security. Contractor shall continually evaluate new technologies and vendor roadmaps so that the most secure and reliable system with the highest performance is available to the County. The Contractor Service Desk shall post text-based information into Tier 0 repositories, and the Contractor network team looks forward to working with the County to advance into video-based Service Desk files in order to better reach Contractor's customer support community.

Hardware associated with remote access shall be refreshed on an ongoing 4-year cycle. This approach shall be continually reviewed with the County, making certain that the refresh activities bring the greatest value to the County while offering continuous improvement to the service.

On a continual basis Contractor shall create, maintain, and update End-User training documentation and tips as well as associated Service Desk scripts pertaining to the remote access to match the version and features of the product.

To allow the maximum return on the County's investment, Contractor shall make full use of the existing solution set, which can adapt to the County's future requirements. However, as the technology and requirements landscapes evolve, Contractor's SMEs shall evaluate and propose new solution sets as needed to meet the County's needs and joint objectives

Network persistence and application persistence in Remote Access Services.

In support of the County's vision of a "Government without walls," Contractor shall maintain a remote access solution that leverages redundant infrastructure with software enabled network and application persistence. This multiplatform solution was designed and delivered to meet specific business purposes, starting with the functionality of SSL VPN and then expanded to provide application persistence for mobile users that actively interact with enterprise data while physically in motion and in turn are exposed to the connectivity interruptions that can occur across carrier mobility networks.

Contractor shall maintain the Pulse Secure SSL VPN service.

As remote access technologies continue to evolve, Contractor shall consolidate the network and application persistence.

User experience, impact to business associated with a change in solutions, as well as providing the proper levels of support shall be carefully weighed for any and all solutions under consideration.

Contractor's approach is to take a transformative approach to this goal, evaluating the best options for the County in the term of the agreement. Contractor shall continue to closely monitor industry trends, vendor roadmaps, and innovation in the remote access space to properly evaluate and select the best solution for the County. Contractor shall work closely with vendors to determine the optimal solution in terms of reliability, usability, functionality, features, and the ability to make full use of the redundant network architecture to preclude any single points of failure as part of the solution.

5.7. Voice Services

5.7.1. Process and Procedures

Voice Services

Each transformational activity shall be initiated through the Enterprise Architecture Forum, where Contractor shall provide ongoing architecture and management resources to facilitate the planning of upgrades, refresh, and strategic plans related to Contractor's voice services. In this forum, Contractor shall perform the following:

- Maintain ongoing collaborative voice and unified communications roadmaps and architectural standards, with yearly reviews/revisions, enabling the continued advancement and adoption of emerging technologies.
- Identify single-point failures within the voice architecture and propose solutions for County consideration.
- Make recommendations to reduce County usage costs.

VoIP Services

Contractor shall leverage the existing network infrastructure and build upon it by replacing older TDM and PBX technologies with Voice over Internet Protocol (VoIP) solutions that tie seamlessly into capabilities already implemented on the County network. As with other transformations, service changes must be completed within realistic cost constraints that provide demonstrable return on investment. Due to these real-world restrictions, Contractor's solution includes significant reuse of existing assets that are current technology and well inside of the technology refresh cycle. Contractor shall reuse the major core voice-related appliances and associated licenses shown in the following table.

Major Core Voice-Related Appliances and Associated Licenses

AVAIL	IN USE	TYPE	DESCRIPTION
26,305	23,901	Aura Communication Manager-Core	Core license for CM stations
26,305	166	EC500	Extension to cellular
26,305*	277	One X Communicator	Softphone on desktop
26,305	0	One X Mobile	Softphone on mobile device
26,305	1	One X Communicator for Lync	Softphone on desktop for Lync integration
2,647*	2,647	Call Center Elite	Core call center software license
321	284	Elite Multichannel	Software for screen pops at ACCESS
484	452	Avaya Call Recording	Software for recording/ storage of agent/ customer voice calls
1,051	2,883	Call Management Agent	Per agent license for CMS
125*	309	Call Management Supervisor	Per supervisor license for CMS
12*	9	One X Agent	Desktop client phone for agents
175*	175	AAEP port	Experience Portal port license
181*	181	AAEP CM Connection	Experience Portal to CM connection license
82*	82	Enhanced Call Classifier	Experience Portal call classifier license
117*	117	Nuance ASR	Experience Portal speech recognition license
117*	117	Nuance TTS	Experience Portal text to speech license
1,000	481	Mutare EVM	Mutare voice mail to email
1,000	481	Mutare giSTT	Mutare voice mail to text transcription
17,000	16,941	Modular Messaging	Voice mail licenses

AVAIL	IN USE	TYPE	DESCRIPTION
26,305	200	Session Manager SIP connections	SIP licenses
3,758	200	Session Border Controller Trunk	SBC licenses for SIP connections
3,758	2	Session Border Controller Stations	SBC licenses for SIP connections

To support Contractor's transformational objective for VoIP services, Contractor's SMEs shall work within the architecture forums and draft Solution Design Documents for the site Transformations. Contractor's formal solution design approval shall then be used by its project management team to develop implementation strategies and communicate with site-based County resources to upgrade each specified facility to VoIP services. These changes reduce equipment footprint at each of the sites, while dramatically reducing the overall power consumption and increasing availability and reliability. Equally important, the upgrade improves the End-User experience by reducing trouble tickets regarding set-based issues—such as speaker and cord problems—and also provides new feature sets.

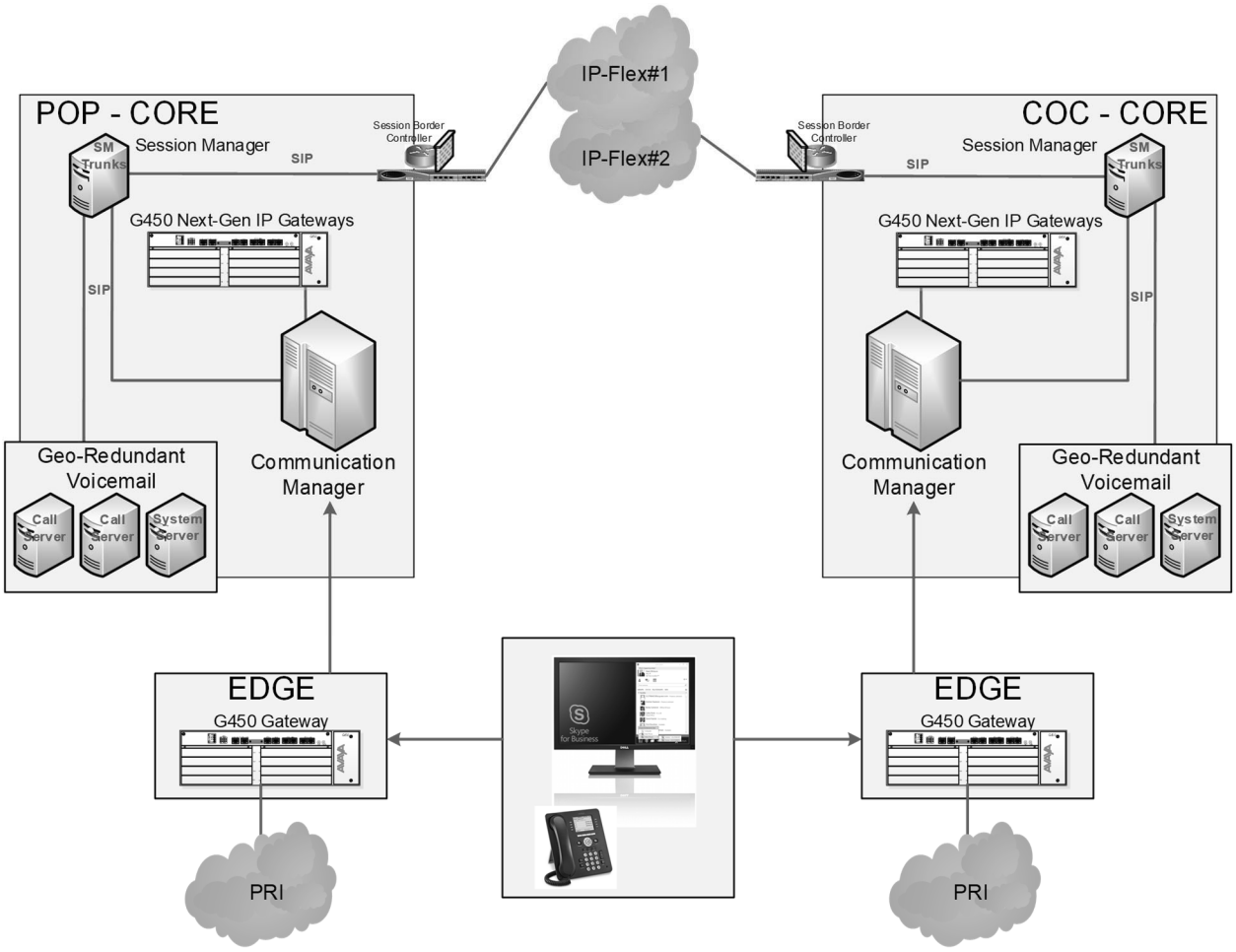
As a part of this Transformation project, each site shall also be migrated to a new E911 service, so that first responders have the necessary site and call location detail in the event of an emergency.

All new County sites shall continue to be implemented with VoIP services as part of Contractor's ongoing efforts to continuously maintain technical currency and modernization of these services.

Geo-redundant Voice Mail

Contractor shall leverage a geo-redundant voice mail platform to provide a standardized voice mail experience across all County locations where enterprise voice services are offered. This solution shall include a phased migration of Centrex users to the new platform as these services are brought into new voice services standards. The following figure is a representation of the high-level topology of the voice mail solution that shall be in place at the time of the Agreement if approved.

High-Level Topology



AVST with Neverfail provides geo-redundant, high-availability voice mail services.

Voicemail to Email Services

Contractor shall continue to support Mutare speech-to-text service for transcribing voice mail messages into text with delivery to the End-User via email along with a .wav file to the County End-User email on a per-request basis by the County. This service is provided via a cloud-based platform.

Unified Communications

Contractor's team shall expand the integrated desktop and handset functionality as part of Contractor's efforts to integrate voice services into unified communication services. These enhancements shall include complete call control from the Lync or Skype for Business client with the following key features:

- Click to call and click to answer from Lync or SfB
- Search and click to call from Outlook contacts
- Outlook contacts match and screen "pop" click-to-conference.

Avaya Communicator Softphone

Contractor shall offer Avaya Communicator softphone functionality. This service allows remote and teleworkers a full featured software client, deployed upon request to their County provided device. Leveraging the

connectivity provided by a direct LAN connection or PulseSecure VPN/Netmotion, Avaya Communicator allows End-Users to make and receive calls from their designated County telephone number at their desk and remotely via a headset.

On-net Dialing and SIP Trunking

Contractor's solution to voice interconnectivity shall use the robust, fault-tolerant solution deployed within the data network to provide resilient connectivity not only within the County domain, but as needed to support cloud-based solutions. This connectivity facilitates improved end-to-end collaboration and also reduces operational costs by implementing efficient local and long-distance dial plans. Contractor shall include capacity expansion of the existing SIP-trunking internally and externally for increased efficiencies. As an immediate objective, Contractor's team shall expand the capacity of SIP services, configuring them to support not just local calls but also long-distance and toll-free (800) calls. Contractor shall eliminate usage charges for all outbound domestic calls from the enterprise and reduce the usage charges for toll-free 800 inbound calls.

Centrex Migration

AT&T has developed a Transformation approach to migrate a majority of these users/stations to a VoIP solution, while maintaining a roadmap for remote and intentionally off-net services to be executed over the term of the Agreement. This effort is planned for implementation early in the term as a Transformation initiative and is included in the Voice Services.

The first transformational step to migrate Centrex users shall include the deployment of stand-alone IP-based telephones at sites with existing data network functionality. This solution provides VoIP telephone sets at the remote site, centrally managed by the Avaya geo-redundant voice cores at the AT&T POP and County Operations Center. While these sites do not have local survivable gateways, they take advantage of the data network for their connectivity to the enterprise voice infrastructure. Through this migration, individual stations shall be converted to the Avaya enterprise standard, where they are provided new centralized voicemail and Unified Communications functionality options as well as a new telephone set.

Basic/Simple IVS Solutions

Contractor shall provide the support of Auto Attendant and Automated Call Distributor services as a right to use feature for subscribers of Voice Services. This basic functionality is inherent to the Avaya enterprise telephony network. Contractor shall enable 39 previously billed "Simple" IVS resource units to consume the service no additional charge.

411 Operator Services

In 2015, AT&T upgraded the IVR that supports the County 411 information line, providing additional self-help capabilities and bilingual voice recognition. This new service has provided improved efficiency in delivering County and public users with County information. Contractor shall continue to provide these services, including a live operator option for users and constituents who "zero" out of the IVR. Over the life of the Agreement, additional recommendations shall be developed and proposed to enhance and improve this important service.

800 Toll-Free Services

Contractor shall ensure that toll-free services for publicly dialed County telephone numbers are supported by AT&T and provided at a significant price reduction relative to current rates.

- Key methodologies and processes in solution including year-to-year continuous improvement

For End-User support within the new contractual service level requirements, the Contractor team shall continue its multi-tiered service and support structure. This structure provides the appropriate skills at each level to handle incidents, coupled with a clearly defined escalation management process to facilitate proper incident response and resolution. In addition, Contractor shall use a complete set of automated tools, which drives quicker response and resolution and minimizes impact.

Each platform/service type shall use a predefined set of operational processes to achieve customer satisfaction and service levels. The Contractor team shall leverage the Nectar Unified Communication Management Platform to access knowledge modules to assist with identifying and resolving issues. Also, Contractor shall leverage an internal SharePoint Services Knowledge Base that provides a customized set of knowledge and process tools specifically reshaped over time for Contractor's internal use only to support voice service response team. The Contractor team shall maintain its voice-specific internal SharePoint Wiki that has complete infrastructure documentation organized by site.

5.8. Network Security Services

5.8.1. Process and Procedures

Network Security Services

- Description of solution to meet the requirements

Contractor shall leverage the existing security infrastructure solution to further improve the security posture of the County network. The following components shall be included in Contractor's solution:

- **Palo Alto next-generation firewalls with unified threat management capabilities.** These appliances provide not only firewall services, but they also provide intrusion detection/prevention (IDP), spyware and AV filtering, and web content filtering. Automated, daily threat updates allow the County network to be protected against the very latest in malicious content and activities. Extensive reporting in this solution enables deep dive views of network communications to highlight the possible effects on network performance. This solution also provides automated alerting of possible malicious activity for immediate investigation and remediation.
- **Websense cloud-based content filtering.** This technology further protects County assets, even when outside the County domain. By replicating content-filtering policies in use on the local County network to the cloud-based service, Contractor is able to support continuity of protection across all avenues of connectivity in use by County personnel, regardless of their physical locale.
- **Websense Data Loss Prevention (DLP) for web channel and data in motion.** This service prevents sensitive data (personally identifiable information [PII] for instance) from being transmitted outside of the County network in unencrypted communications or copied to a removable device (i.e., thumb drive).
- **Advanced Distributed Denial of Service (DDoS) detection and protection.** This service protects County Internet circuits and provides security event analysis and correlation via live 24x7x365 monitoring.
- **Tenable Security Center.** Continuous perimeter scanning provides a close to real-time view of supported and non-supported inventory, including real-time threat updates and monitoring of vulnerabilities and risk, as well as close to real-time asset status updates. This provides an improvement to the snapshot in time information that is currently available.

Transformation Opportunities

As part of Contractor's dedication to continuous improvement for the County, Contractor shall support and maintain the following efforts:

- **Application-level security policies.** By moving from port/protocol-based firewall policies to application-based policies the tools can fully inspect traffic flows. This type of technology safeguards against programs attempting to use non-standard ports to circumvent port/protocol-based security. The Contractor team may refine security policy to data flows, as well as determine the types of applications in use on the County network. This enables Contractor to provide more in-depth assessments and recommendations for network enhancements.
- **User identification.** By providing positive identification for each End-User tied to a data transmission, firewall policies can be written to allow authorized network communications based on End-User ID rather than an IP address. Consequently, the policy is in effect for the End-User, regardless of his or her location on, or entry point into, the County network. This solution eliminates the need for static IP addresses for firewall policy mapping—thereby providing better policy management without the need to map policies to entire subnets to accommodate the mobile nature of today's workforce.
- **Active Directory group-based policies.** Much like End-User identification, AD-based policies allow for the mapping of security policies to specific groups created within AD. This allows for a security policy to be applied to all users who are members of an AD group, regardless of where they reside on the County network. For example, if a member is added to the HR group then he or she automatically inherits the security policies applied to that group without having to have a firewall change made to accommodate him or her specifically. As a result, Contractor's SMEs have greater flexibility in mapping security to End-User roles without increasing complexity in either process or implementation.
- **Network Access Control (NAC).** This capability provides appropriate levels of network access based on the device being connected. County-managed devices are given full access to the County network just as they are today. Non-County devices are segregated on the County network and allowed only access to the Internet unless otherwise authorized through a formal review process.
- **Integration with the County's PKI solution.** These integrated solutions guarantee that only County-authorized devices are able to connect using County wireless networks or via the County's SSL VPN solution. This approach effectively isolates the network from exposure to non-County managed devices that pose a security risk.
- **Websense Data Loss Prevention (DLP).** The DLP solution is already in place for data in motion and web channel, protecting against the release of sensitive data onto the public network or transfer of data to removable devices. The next phase of that enables the scanning of repositories to identify sensitive data being stored in non-secure locations.

- Deployment plan for resources and use of facilities

All hardware and software used to provide network services from the AT&T POP location shall be contained in a secure location, accessible only by AT&T personnel or those they escort. All personnel having access to County associated devices at the AT&T POP shall have undergone background checks and verification. Security measures shall include guarded access, with signature and ID required for admittance along with biometric security.

Access to network services hardware and software located at County facilities is to be managed by the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall evaluate patches and updates as they are made available to determine their applicability to the County environment and shall deploy them immediately as needed.

The continuous 4-year refresh cycle shall apply to security hardware as it does to all network refresh activities. The hardware and systems shall be continuously evaluated so that they can meet the requirements of the County's high-speed network and are upgraded as needed.

Contractor shall perform the configuration of the hardware and software using industry best practices—resulting in hardened, or locked down, systems. Contractor shall remove default usernames and passwords and disable

unnecessary services, and all management communications to and from the devices shall be via encrypted connections.

- Use of Tools

Contractor shall provide and maintain a centralized management platform to deliver strict change control along with powerful reporting and alerting capabilities and automated notification of security events.

Through AT&T's vendor, Security on Demand, Contractor shall capture these threats by performing analysis against the data, including behavioral analytics, to determine whether there is a potential threat. If such a threat exists, or further analysis with the LCM team is required, then a ticket shall be generated or a call placed directly to Contractor's dedicated security staff for high severity issues.

The logging mentioned above, as well as all of the logging from the Contractor security devices, shall be fed into the security information and event management (SIEM) solution for analysis and triangulation against other security data sources such as data center firewalls and intrusion prevention systems/intrusion detection systems (IPS/IDS).

Automated email alerts shall also be delivered daily to the dedicated Contractor security staff by Contractor's Palo Alto environment, where additional analysis shall be conducted and fed to the Cross Framework security team and Cross Framework capacity and performance team. Finally, Contractor's Security team shall use these tools to develop recommendations for evaluation by the Contractor CISO and County CISO.

From this analysis, Contractor shall take actions to include, but not be limited to, scanning of devices, removal from the network and reimaging of desktop devices if necessary (for County assets), and configuration of network or URL blocking and tuning of threat signatures. Contractor shall conduct investigations to determine whether hosts have fallen victim to malicious activities and what the impact or spread of those may be. All investigative reports shall be provided to the County for its review.

In addition, monthly reporting shall be provided to the County CISO for review with PMO Security on both threat alerts and URL blocking taking place in the County environment. This allows both trending analysis and the development of future security strategy roadmaps.

5.9. Video Conferencing Services

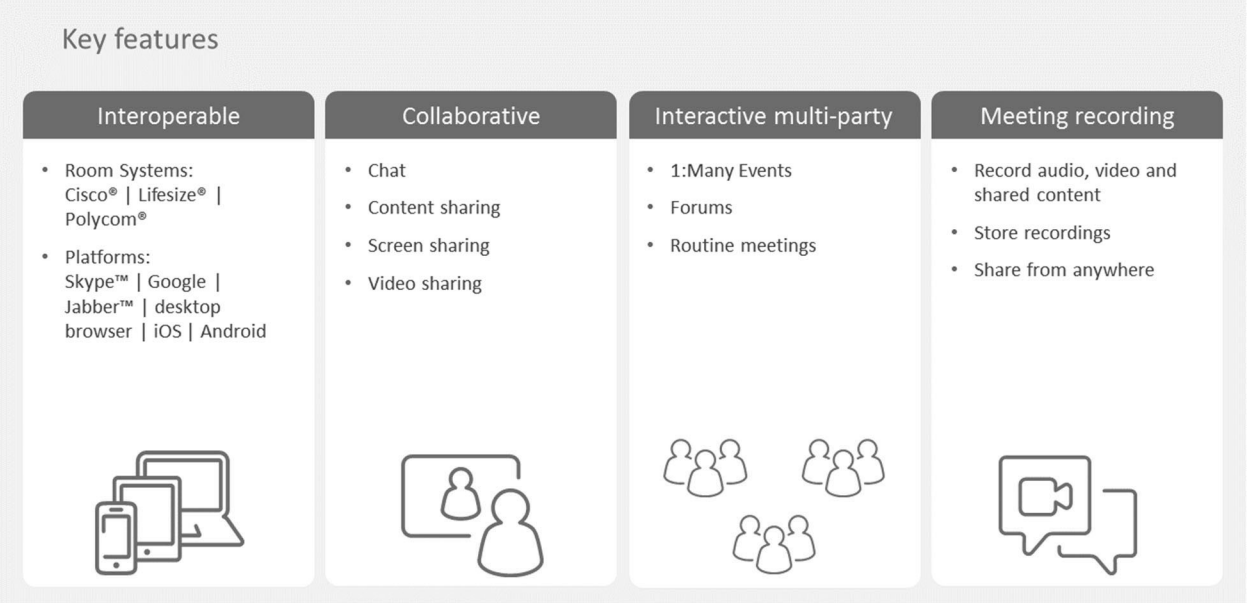
5.9.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall continue the use of existing video conferencing capability in conjunction with a cloud-based solution to fulfill all of the County video conferencing requirements. To remain compliant with required equipment refresh cycles, part of Contractor's solution replaces the Tandberg Management System (TMS) and Video Conferencing System (VCS) with the Cisco Unified Communications Manager (CUCM) virtualized appliances, which shall be implemented in a geo-redundant configuration between the AT&T POP and the County Operations Center.

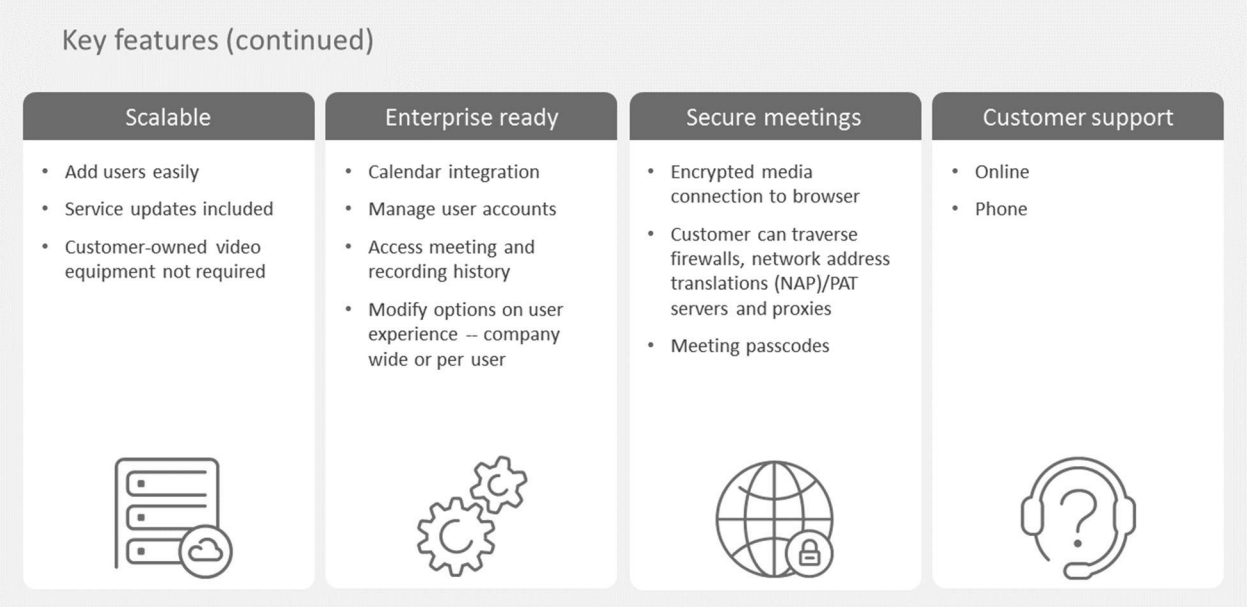
To fulfill the need for a fully integrated video teleconferencing solution, Contractor shall provide AT&T Meetings with BlueJeans. This solution offers a cloud-based video bridging capability that can integrate services like Skype for Business and Google Chat with traditional standards-based room video systems. The system is scalable, device and platform agnostic, and provides a flexible yet standard platform for video teleconferencing. Features of this integrated solution is depicted in the figures below.

BlueJeans via AT&T



The hosted Meetings with BlueJeans via AT&T provides full interoperability across many platforms and allows for many types of collaborative, real-time interaction.

Hosted Meetings with BlueJeans via AT&T



The hosted Meetings with BlueJeans via AT&T scales easily both internally and externally, while providing additional enterprise and security capabilities.

This Meetings with BlueJeans solution leverages the availability of existing videoconferencing units around the County and facilitates interoperability with the existing Skype for Business clients for extended telepresence. Users can participate from anywhere using any device—with a dedicated app, a web browser, or the Skype for Business mobile application.

From a desktop/laptop/tablet/smart phone End-User's perspective, the Meetings with BlueJeans experience is as easy as clicking on a link in an email or a meeting request. The Outlook plugin adds the capability to schedule meetings using a personal meeting ID or a dynamic meeting ID. Users can also edit default meeting preferences and add/edit/cancel meetings. The additional support for delegate scheduling allows executive support personnel to schedule meetings on behalf of executive staff. From an existing Cisco videoconferencing unit, an End-User simply dials by inputting the IP address as listed in the invitation.

Additionally, the Meetings with BlueJeans hosted solution allows numerous customizations, including the ability to set language preference, meeting passwords, entry tones, meeting security controls, and more via the web-based End-User interface. Features such as the high-definition content support, video sharing, and the ability to record meetings coupled with the integrated encryption allow the County to conduct video meetings securely as desired today and into the future.

- Deployment plan for resources and use of facilities

Contractor's solution shall use the existing video conferencing solution set and the associated facilities that house the equipment, including core infrastructure in the AT&T POP and the County Operations Center. Furthermore, Contractor's existing local staff shall continue to support the video conferencing services as well as all of the other framework components from its County location. This local staff shall also be responsible for continuous development, maintenance, and updates of all items associated with video conferencing, including Service Desk scripts, training documentation, and processes for End-User support—and this staff shall continually provide new and updated material to support operational needs.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's SMEs shall continue to evaluate solutions and introduce them through the weekly network architecture meetings and thereafter through the Enterprise Architecture Forum. These iterative processes allow Contractor's solutions to address known and projected business requirements, convey direction, gain insight regarding other project path implementations, and allow required approvals as well as maintain consensus.

The Contractor team shall use insight gained from the ongoing operation and maintenance of the infrastructure to assess potential transformational, refresh, and upgrade activities. If other SPOFs are identified and remediated, then Contractor's SMEs understand the processes and documentation to effect the change with minimal effort by all parties involved. Contractor's local, dedicated team provides the coordination of resources necessary to plan, design, and implement the video and archiving solution.

When Contractor receives an Install/Move/Add/Remove (IMAR) request, it shall gather information and design a solution to present for the County's approval. Once approved, Contractor shall order, receive, and stage the equipment and other necessary components for installation. Contractor shall coordinate the installation date with the End-User or business unit and dispatch a technician to complete the installation.

The BlueJeans integrated video teleconferencing solution shall include a 100-host license, where designated video conferencing hosts are to be identified by the County. These 100 licenses represent simultaneous conferences, as only one licensee is required per conference. These licenses are dynamic and can be changed in real time to different users via the scheduling portal.

Over the life of the term, the wider adoption of standards-based systems like Skype for Business/O365 along with anticipated industry enhancements may shift the solution for multi-platform video teleconferencing. The Contractor believes that the Microsoft's planned development of multi-platform transcoding via a Skype for Business mediation server positions the County to move towards a Skype based standard for all video teleconferencing services. The Contractor shall work with the County to evaluate such options and make recommendations accordingly.

Integration of desktops into Video Conferencing Services.

Contractor shall provide AT&T Meetings with BlueJeans, a hosted video bridging capability that can integrate services such as Skype for Business and Google chat with traditional standards-based room video systems. This enables fully integrated business-to-business (B2B) video calling and is scalable, device and platform agnostic, and provides a flexible yet standard platform for video teleconferencing.

Additionally, as the County increases its use of video teleconferencing, AT&T NetBond enables videoconferencing traffic to be redirected off of the ISP connections to a private multiprotocol label switching MPLS connection to support additional performance, scalability, and security above and beyond the integrated encryption. The NetBond to BlueJeans cost is not included in the Baseline Resources Units.

BlueJeans users can also benefit using Outlook plug-ins. An End-User can schedule meetings using a personal or dynamic meeting ID, edit default meeting preferences, and add, edit, or cancel meetings. Delegate scheduling provides administrative staff the ability to schedule meetings on behalf any team member. To set up a call, the End-User simply inputs the IP address as listed in the invite.

The BlueJeans platform allows numerous customizations including the ability to set language preferences, meeting passwords, entry tones, and meeting security controls via the web-based End-User interface. Features like high-definition content support, video sharing, and the ability to record meetings, coupled with the integrated encryption, provide secure meetings for County users.

5.10. Video Streaming and Archiving Services

5.10.1. Process and Procedures

Video Streaming and Archiving Services

- Description of solution to meet the requirements

To support the increasing video distribution needs of the County, from both live and on-demand perspectives, Contractor shall use the existing Granicus System as a compliant starting point. This provides continuity and stability as more future-focused technologies are investigated.

- Deployment plan for resources and use of facilities

Contractor shall use the two current core facilities already in use at the AT&T POP as well as the CAC as a primary video content sourcing location. Furthermore, this solution shall use the existing network infrastructure to support an efficient video distribution capability. Contractor's local, dedicated staff shall be active liaisons on behalf of the County, and Contractor shall select external cloud providers so that required service level requirements are continually met.

- Key methodologies and processes in solution including year-to-year continuous improvement

Going forward, Contractor shall achieve consensus on the Video Streaming and Archiving Services Roadmap by vetting or via recommendations in the weekly network architecture meetings—and thereafter via the Enterprise Architecture Forum. Use of these iterative processes allows Contractor's solution to address known and projected business requirements, convey direction, gain insight regarding other project path implementations, and allow required approvals while maintaining consensus. As such, Contractor's SMEs shall continue their active participation within these forums as well as their participation in other meetings to stay abreast of customer needs, report on changes in technology, and propose low-risk solutions to meet County business requirements. Furthermore, the Contractor team shall use insight gained from the ongoing operational and maintenance aspects of the infrastructure to assess potential transformational, refresh, and upgrade opportunities. Contractor's local, dedicated team shall provide the coordination of resources necessary to plan, design, and implement the video and

archiving solution. All work efforts and problem reports shall flow through the existing processes in place for support of the County's network by the AT&T LCM team.

On a continual basis, Contractor shall create, maintain, and update End-User training documentation and tips, as well as associated Service Desk scripts pertaining to the solution, to match the version and features of the product.

- Use of Tools

As new appliances and capabilities are expanded within the existing data network, the Contractor team shall expand the use of CA Spectrum and eHealth to monitor the operational status of the appliances and the bandwidth usage so that the ongoing operational capabilities are met as compared to the service level requirements. High-grade analytics shall provide viewer statistics along with performance information to provide a clear picture of performance and where possible trouble spots within the infrastructure may be occurring so that Contractor can take near-real-time corrective actions.

5.11. Mobility Infrastructure Services

5.11.1. Process and Procedures

Mobility Infrastructure Services

- Description of solution to meet the requirements

AirWatch MDM Infrastructure

All components of Contractor's industry-leading AirWatch Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for the County shall be maintained and supported in a fully geo-redundant configuration. The AT&T MDM solution shall use a cloud-based AirWatch Software as a Service (SaaS) MDM/EMM solution integrated with on-premise AirWatch Cloud Connectors (ACCs) deployed into the AT&T POP and the County Operation Center. These ACCs in turn shall interoperate with the County's Active Directory infrastructure for End-User authentication.

Contractor shall maintain and support its proxy services between County Enterprise Systems and the SaaS MDM/EMM cloud, as well as application gateways services for developed or acquired applications, to internal County resources from mobile devices using Mobility Infrastructure Services.

Due to the nature of the cloud service and the geo-redundant configuration of the on-premise infrastructure, the AT&T MDM solution has no identified single points of failure.

Mobile User and Device Profiles

Contractor shall maintain and support the three profile groups established within AD: The Corporate Single Device, the Corporate Multi Device, and the Bring Your Own Device (BYOD). These profile groups can be expanded as business needs are defined, where the Contractor team simply adds a group profile within AD recognized by the AirWatch Platform. Users are identified through CSRFs and placed into the respective groups.

Contractor shall support County "corporate owned" devices and BYOD in a reliable and secure manner and shall manage them according to specific County-defined policy.

After being enrolled within the designated group, when a mobile device End-User requests access to the County domain, the End-User is certified against the AD; thereafter three profiles (Passcode, Restrictions, and Exchange) are pushed Over the Air (OTA) to the device.

The AirWatch cloud-based solution provides central management and control of all mobile devices and mobile applications from a single unified console. This console also allows Contractor's solution to enforce County-approved device policies for security and data protection across the End-User population of County and BYOD mobile devices. For instance, Contractor's solution provides the County Mobile Application Store for developed or acquired mobile applications and limits the access to the applications to only County-managed MDM devices.

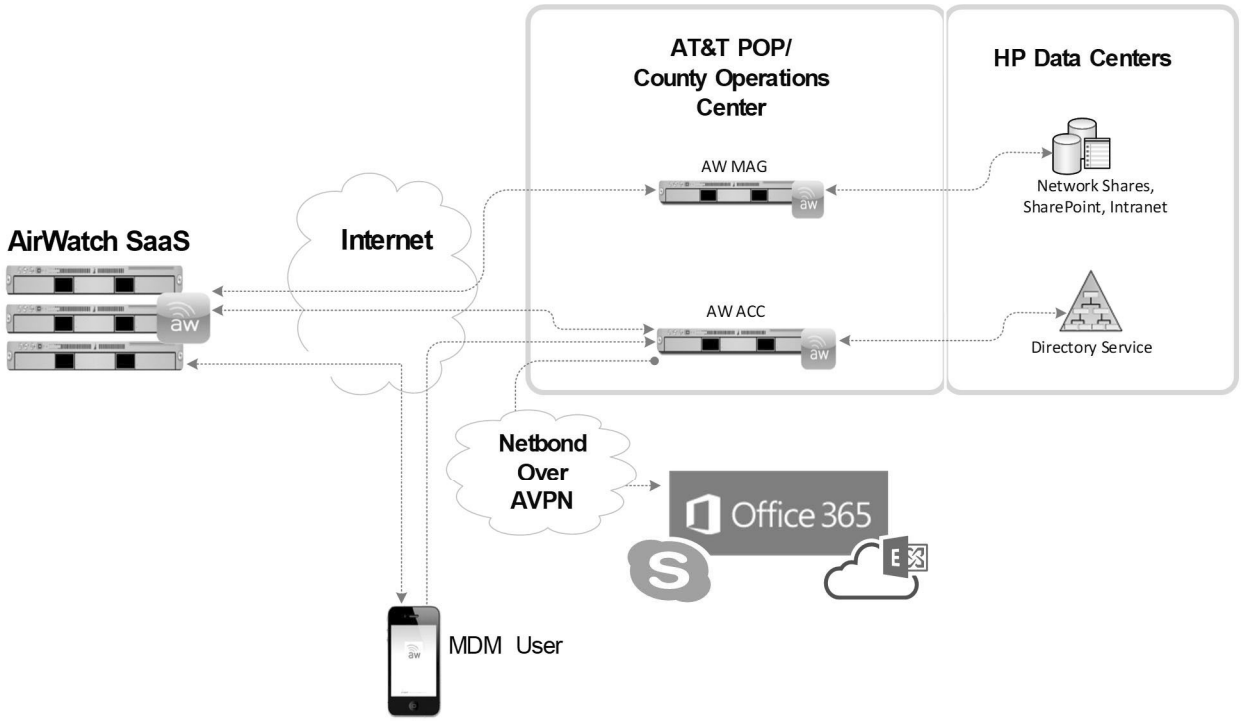
Mobile User and Device Authentication

Contractor's solution shall enable client authentication, encryption, and message signatures to secure corporate resources and connections. AT&T's SaaS MDM/EMM solution shall integrate with third-party Certificate Authorities and Public Key Infrastructure (PKI) providers in cloud and on-premise deployment models. AT&T's SaaS MDM/EMM solution shall distribute Symantec Managed PKI certificates to corporate managed mobile devices for mobile VPN authentication and integration. Future roadmap capabilities shall include the potential for PKI integration delivered via AirWatch MDM for access to County staff Wi-Fi as well as seamless integration with the PulseSecure Mobile VPN application.

AirWatch Integration with O365

As a Transformation initiative, Contractor plans to migrate Exchange to the O365 cloud. Although the current integration from the AirWatch SaaS MDM/EMM solution to the County infrastructure for email services is premises based with integration to services in the data center, the solution can be configured to integrate to Office 365 with Outlook via an AVPN with AT&T NetBond service. Contractor shall ensure that AT&T and its Mobility Solution Services team engages in this migration effort, updating design documentation and making certain that End-User connectivity to email is enabled as the services are migrated to the cloud. The figure below presents the reconfiguration of the AirWatch premise-based infrastructure.

AirWatch



The AirWatch premise-based infrastructure is reconfigured as part of the migration of Exchange to the O365 cloud, enabling email access to MDM-compliant devices.

- Deployment plan for resources and use of facilities

Contractor shall use the existing, knowledgeable AT&T Lifecycle Management team located at 7337 Trade Street in San Diego, California, along with AT&T's leveraged Mobility Support Services (MSS)/Application Service Desk (ASD) organization to continue to support the premise- and cloud-based AirWatch infrastructure.

The ASD is composed of experienced, industry-certified professionals who provide hands-on, comprehensive, and proactive managed services and technical support. In addition to the ASD, the local team also retains a highly skilled mobility consultant, who has intimate knowledge of the County AirWatch tenant and continually provides support and guidance on operational and strategic initiatives.

Facilities involved shall include an AT&T POP in the County as well as the County's Operations Center.

- Key methodologies and processes in solution including year-to-year continuous improvement

The SaaS MDM/EDM solution shall include the following key processes:

- User acquires phone and needs access to County resources.
- A request is made for access via an Install/Move/Add/Remove (IMAR) through Contractor's Service Desk.
- User goes to the public apps store and downloads the MDM/EDM application.
- The Contractor team processes the request and gives permissions for allowed systems for the End-User.
- User enrolls into the MDM/EDM system via an End-User guide provided by the Contractor team.
- Any issues are directed to the Service Desk.

Contractor's MDM service shall require a monthly RU and a one-time upfront fee per End-User at the time a new End-User subscribes to the service. The one-time fee includes licensing costs.

Contractor shall participate as dedicated resources supporting upgrades, refresh, and transformational activities related to mobile infrastructure services. Contractor's SMEs shall continue to use Pilot Charter and Solution Design Documents as well as other documents and briefings to convey Contractor's recommendations for County review.

To stay up to date Contractor shall conduct quarterly collaborative reviews of mobile device standards, including hardware and operating systems, for incorporation into the Standards and Procedures Manual for Standard Mobile Devices. Furthermore, the Contractor team shall use the approved Standards and Procedures Manual when developing standards for all mobility infrastructure services that are submitted for approval on a semi-annual basis. Contractor shall conduct quarterly updates to the timeline/roadmap of all mobility infrastructure services hardware and software version life cycles so that responsive time frames and completion dates stay within supported versions of hardware and software.

5.12. Wireless Network Access Services

5.12.1. Process and Procedures

Wireless Network Access Services

- Description of solution to meet the requirements

Contractor shall manage a comprehensive wireless architecture that provides services to County staff and constituents. Contractor's solution shall provide wireless services for managed computing assets on the secured County internal wireless LAN as well constituent and guest assets on a public Wi-Fi infrastructure. This wireless infrastructure shall consist of centralized geo-redundant controllers, wireless access points, various software-based management tools, and security components.

Wireless Infrastructure

Contractor's two centralized wireless LAN controllers shall provide redundancy and resiliency through high-availability, geo-redundant configurations that leverage diverse facilities (AT&T POP and the County Operations Center). These controllers shall maintain Contractor's centralized configuration, act as a single point of interface for changes and monitoring, and support a variety of access point models.

Contractor shall maintain and support the 380+ wireless access points throughout the County to provide wireless connectivity for the End-User. The Contractor team has standardized on the Cisco 3702 for wireless access within County facilities, whereas for outdoor areas Contractor has standardized on the Aruba 274/5. Both products shall continue to provide support for legacy connectivity, such as 802.11 A/B/G/N as well as the new 802.11AC standard. This wide range of support shall allow all Wi-Fi capable devices, regardless of age, to obtain connectivity through the County wireless infrastructure.

The Contractor team shall continue to use several software suites to provide visibility deep into the operations, planning, and support of the County's wireless infrastructure. These tools include management tools, such as Airwave and Cisco Prime Infrastructure, as well as survey tools such as Fluke's Air Magnet.

Wireless Network Authentication

For County secure wireless, the Contractor team has worked with desktop support services at Contractor to deliver a certificate to all managed devices required to authenticate via EAP–TLS and connect to the County's secure wireless infrastructure. Contractor shall continue to provide public access in various County locations, such as the libraries, and shall be segregated logically and physically. Additionally, Contractor shall use its next-generation firewall infrastructure, including content filtering functionality, to provide the most robust security available for the wireless infrastructure.

This architecture, coupled with an NAC and PKI initiative, shall serve to further increase the security posture of the wireless infrastructure. By leveraging these capabilities, additional controls shall be enabled, providing seamless access to wireless staff users, while redirecting untrusted/unmanaged assets to a guest access portal via a splash screen, where they can then obtain public network connectivity. This architecture shall support a closed loop system whereby only known, managed assets shall be able to connect to the secure wireless infrastructure, with little to no additional interaction from the users to facilitate this additional security.

- Deployment plan for resources and use of facilities

The local, dedicated LCM team shall provide all design, implementation, support, monitoring, and reporting of all wireless network services.

Core infrastructure for the wireless network shall be housed at the AT&T POP and County Operations Center, which shall provide secure, restricted access. Wireless access points shall be installed upon request in County facilities according to industry and County-approved standards.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's engineering team shall work with County's CTO to evaluate the new and emerging wireless standards and their enterprise readiness. Contractor's recommendations shall take into account not just the performance of new wireless access points, but also the device standards being used by County End-Users, so that the timing of the investment enables the largest population of users to take advantage of the advancements.

When a recommendation is approved, the Contractor team shall move forward with project management processes, including planning, scheduling, and implementation of the refresh of existing equipment as well as other infrastructure changes.

For equipment issues, the Service Desk and engineering team shall work to identify and remediate the problem.

5.13. Third-Party Network Access Services

5.13.1. Process and Procedures

Third-Party Network Access Services

- Description of solution to meet the requirements

Contractor shall use the existing solution sets in response to expanding business requirements to support third-party access to and from and across the County data network. Overall, three different types of support shall be provided:

- Dedicated leased line connectivity
- IPSec connectivity
- Virtual circuit support.

Each of these solution sets play a vital and specific role in supporting various County business areas. The solution used for access is based on the location of the third-party devices, the type of communication required (system-to-system versus End-User interactive session), the tolerance of bandwidth variations, and latency impacts.

Using the Third-Party Access Request (TPAR) process, Contractor shall determine the required connection types and any details necessary to provision the access. This process shall identify the specific third-party devices, the County resources being accessed, and whether the communications occurs over the internal domain and/or open Internet. This information shall be used to create strict firewall policies so that only the approved devices and resources are accessed for use by the third parties.

Contractor shall provide unified threat management technologies to include intrusion detection and prevention, virus and malware filtering, firewall security policies, monitoring, and reporting for these third-party connections. All data traverses the County's next-generation firewalls to enable full visibility into all data flows up to and including the application level. All data classified as sensitive and above shall be encapsulated in a secure tunnel as it egresses the County network, regardless of its point of origin within the managed network.

Third-party interfaces shall also be included in the LCM team's capacity and performance monitoring services. This approach facilitates reporting on usage and possible impacts to performance resulting from spikes or increases in usage. All access to County resources from third-party users shall be managed via Active Directory and End-User account levels of access.

Contractor shall support and maintain third-party network access models and use cases are as follows:

- **Dedicated Leased Line Connections.** Third-party leased line connections are used to connect the County network to a third-party network via a dedicated transport (i.e., T1, Opt-E-MAN, Opt-E-WAN, and so forth) that is provided by the Third Party. This solution is chosen when throughput must be guaranteed because the dedicated circuit is not impacted by fluctuation in utilization of public Internet circuits. A dedicated circuit also provides the highest level of security in terms of confidentiality, integrity, and availability.

IPSec Connections. IPSec provides a secure tunneled connection over the Internet. It encrypts sensitive data and allows machine-to-machine connectivity for scenarios where automated jobs run connections into or out of the County network without End-User interaction. It also provides access into the County network for authorized systems or users without the need to install specialized VPN software on the remote hosts. Virtual Circuits. The virtual circuit design allows placement of non-County devices onto the County network in a way that keeps them isolated from County assets. All communication to and from County resources is still regulated by firewall policies. Presently, this solution supports users within 55 virtual circuits inside the County domain without exposing the network to risk.

As part of the dedicated team's ongoing efforts to provide continuous improvements to, and enhancements of, all frameworks for which they are responsible, Contractor shall continually look for alternative solutions that benefit the County's voice and data network.

- Deployment plan for resources and use of facilities

The local, dedicated LCM team shall provide all design, implementation, support, monitoring, and reporting of each of the third-party access solutions. All managed hardware in association with such shall be housed at the AT&T POP, which shall provide secure, restricted access as well as fully redundant power. Contractor technical personnel and hardware associated with the County program shall be dedicated to the program.

- Key methodologies and processes in solution including year-to-year continuous improvement

The local, dedicated LCM team shall be embedded in the full life cycle of every third-party access connection—from the initial gathering of requirements, through the design and implementation phases, to managing and monitoring, and even decommissioning when requested. Through customer meetings and security reviews, the team shall evaluate the proper access method so that it is sized appropriately and verifies that all necessary security measures are in place.

Third-party network access options shall be continually evaluated based on County business requirements in addition to current and emerging technologies.

5.14. External DNS Management Services

5.14.1. Process and Procedures

External DNS Management Services

- Description of solution to meet the requirements

The external Domain Name Service (DNS) cloud-based platform, which uses Akamai cloud-based FastDNS service, shall be the basis for Contractor's DNS management service.

The Akamai FastDNS solution shall provide an authoritative DNS service that offloads DNS resolution from the County's infrastructure to the cloud to provide 24x7 DNS availability. It shall be optimized for performance through global distribution and presence and reliability—protecting against DDoS attacks while allowing for additional security through the Domain Name System Security Extensions (DNSSEC) to protect against DNS forgery and manipulation. Contractor shall perform DNS management as required for all of the external-facing County DNS records (A, MX, CName, and so forth) via a web browser that accesses the Luna Control Center. The Luna Control Center is the web-based portal that provides customers with access to—and control of—their Akamai services as well as reporting and monitoring functionality.

Through coordination with the County, Contractor shall fulfill requests to add, move, or change the information published for specific domain name records within the Akamai solution, as well as remove obsolete records to preclude any instances of orphaned or bad records. Although the existing DNS implementations allow a logical separation between the internal and external DNS, Contractor SMEs shall integrate specific elements, as required by the County, subject to essential network security provisions.

Through the use of the Akamai FastDNS service, single points of failure shall be inherently mitigated by the design of the solution. The Contractor team shall regularly evaluate this position throughout the life of the term so that the most cost-effective and technically sound solution is provided to the County.

Also included within Contractor's support activities include the maintenance of a comprehensive roadmap of all external DNS management services required in conjunction with Akamai and the County. This roadmap allows

Contractor to adequately inform its customer and plan time frames and completion dates for any software changes needed to improve service capabilities. As an integral part of these coordinated services, Contractor's SMEs shall facilitate ongoing product and solution strategy planning with Akamai, so Contractor's collaborative roadmaps remain up to date with new and emerging functionality and service changes.

- Deployment plan for resources and use of facilities

The LCM team shall continue to use the Akamai cloud-based resources as an integral part of Contractor's solution. Contractor shall operate and manage the service from its Rancho Bernardo site, where its support personnel shall manage all aspects of the data network to include external DNS support services.

The Contractor team shall leverage some remote resources, such as those from Akamai, and those support activities fall directly within the purview of one or more of Contractor's local SMEs for adherence to the County's requirements.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor staff shall participate in supporting continuous architecture and management activities for the internal and external DNS.

From an external DNS perspective, Contractor shall work to establish new records or remove existing records based on the associated activation or deactivation of new services that tie to an external DNS service.

5.15. IP Address Management Services

5.15.1. Process and Procedures

IP Address Management Services

- Description of solution to meet the requirements

Contractor shall use the BlueCat Proteus Enterprise IPAM v4.0.5-20 Platform as the single user interface providing integrated management of all static and dynamic addresses. Operating within the AT&T POP, this virtualized solution configures and documents changes to the IP address landscape and collects real-time information related to the current IP allocation within the network. A standby platform shall be located within the COC to mitigate against a single point of failure. In turn, the Proteus management platform shall communicate with the BlueCat Adonis appliances that are geo-redundantly located within the COC and the AT&T POP. These appliances shall serve as the policy recipients from Proteus and thereafter monitor, manage, and configure all Dynamic Host Configuration Protocol (DHCP) services within the County's internal network. The Adonis System also relays IP address utilization information back to Proteus for data aggregation, analysis, and presentation, as required.

Due to the inherent capabilities of Proteus, Contractor uses this management platform for a structured approach to IP subnet assignment, to control static IP address use, and to monitor dynamic address allocation. Additionally, Contractor's solution allows IP address data to be collected, analyzed, and organized into the monthly DHCP pool and IP subnet utilization and trending reports for the County. In addition to providing automated discovery of IP addresses, this tool allows Contractor engineers to detect and manage conflicting or duplicate address use quickly so that normal network operations are maintained.

This solution set shall manage and control the network domain using an IPv4 address schema, but it is fully capable of supporting IPv6 when address transformation is required. Contractor shall support the equivalent of 916 Class C address blocks for internal, external, third-party, and public network access through Contractor's data networking services using efficient, fault-tolerant routing so that Contractor's services meet the County-specified service level requirements. The Contractor solution shall be fully and continuously synchronized with the internal

DNS services using the DHCP servers, which provide DHCP clients with the fully qualified domain name and IP addresses for DNS services. Additionally, Proteus provides Active Directory information regarding IP address assignments for System Center Configuration Management (SCCM). Via SCCM, efficient network utilization is maintained by designating Distribution Points (DP) within the domain to service adjacent blocks of IP addresses for system upgrades or patches. In this manner, blocks of IP addresses are automatically directed to the nearest DP, network traffic is localized to the extent possible, and latency is reduced.

- Deployment plan for resources and use of facilities

The LCM solution shall continue to use the County Operations Center and AT&T POP for the reliability and resiliency IPAM services to help the continuity of network in accordance with service level requirements.

Additionally, Contractor shall continue to use the AT&T Trade Street facility to house its local support personnel and manage all aspects of the data network, including IPAM. LCM shall continue utilization of its local team, which has allowed close alignment with the needs of the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's SMEs shall continue to use the weekly network architecture meetings and the Enterprise Architecture Forum to notify Contractor's user community of identified SPOFs or other enhancements and then implement Contractor's approved solutions. Additionally, Contractor staff shall also continue maintaining a comprehensive roadmap of all IPAM services hardware and software life cycles. This roadmap allows Contractor to adequately inform and plan time frames and completion dates to stay within supported versions of hardware and software.

From an IP addressing perspective, Contractor's support methodology focuses on four scenarios that require Contractor staff's intervention to provide the County with timely service:

- **New Site Activation.** Contractor project management personnel are involved in the creation of any new site, and they include IPAM as part of the actively managed project plan. As needed, new block(s) of addresses are allocated for the site, and the recommended DP is also determined.
- **Site Decommissioning.** Contractor project managers are involved in any site decommission, and IPAM is part of the project plan as Contractor recovers existing block(s) of addresses for reuse.
- **Significant site growth projections.** Depending on the scale of growth projected, Contractor project managers shall be involved and include IPAM as a part of the project plan. In contrast, Contractor shall use the IMAR process for smaller projects.
- **Static addresses are required.** To accommodate these requirements, Contractor leverages the existing IMAR process to gain a static IP address, which is issued from a predetermined range for each site defined within the IPAM tool.

5.16. New Site Installation Services

5.16.1. Process and Procedures

New Site Installation Services

- Solution Summary & Rationale – Description of solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

One of the key strategic initiatives for the County has been real estate planning and facility construction for the long term. This has resulted in the design and construction of new, state-of-the-art County sites. Since the beginning of the existing Agreement in 2006, the County has built 87 new locations throughout the region. The majority of these have been Leadership in Energy and Environment (LEED) certified; more than 30 have been

awarded the highest level of LEED achievement. AT&T has partnered with the County and Contractor to help plan, engineer, and build IT infrastructure in all of these locations through the new site installation services component of the Agreement.

The current structure of new site installation services categorizes new sites into tiers based on the number of network access, voice, or VoIP jacks resource units to be installed at each location. This has provided the County with the advantage of predictable telecom infrastructure costs when forecasting the overall financials for facility construction. It has had the disadvantage of restricting the County's flexibility in assigning structured cabling work to vendors other than the IT contractor when circumstances warrant.

To meet the County's requirement for the flexibility to engage its own cabling vendor, the Contractor shall provide a solution that includes base services and optional services within the prescribed End-User based tiers that define the site types. This new RU structure shall consist of 5 RU's by site type, with base and optional services within each.

Base services (the fixed component), shall include activities such as pre-field work and requirements gathering, network design, circuit design/provisioning, installation of network hardware and project management that are required regardless of the cabling vendor used.

The optional services (the variable component), shall include all cabling vendor activities as well as contractor project management oversight. These optional components are broken into two work categories to allow the County to select either all or a subset of the cabling work necessary at the new site. The first component within the optional services shall be identified as "Riser Cabling". This component shall include the placement of pathway and rack infrastructure as well as the placement and testing of fiber/copper based cabling runs between MPOE and MDF, and between MDF and IDF rooms/floors. Trenching is not included in this service and shall be the obligation of the County or their contractor to provide. The second optional component of the service shall be identified as "Horizontal Cabling". Included in this service shall be the placement and testing of all wall jacks, patch panels and plenum cabling between the IDF and the workstations or designated end points.

- Should the County elect to move one or both of these optional service components to a vendor of their choice, the resource unit shall be decomposed to provide adequate cost recovery for the remaining New Site services. For example, in a situation where the County were to elect to do their own Horizontal and Riser cabling at a New Site, the cost of these activities shall be deducted from the overall Resource Unit price and Contractor shall execute the base (fixed component) of New Site activities required to establish connection to the County network. Additional clarity on these fixed and optional services can be found in Schedule 16.1-2. Resource and Facility Approach Summary –deployment plan for resources and use of facilities

Resources that Contractor shall utilize for this effort shall include facility project managers and network design and field engineers. They work out of the Trade Street AT&T facility. This team conducts the design and planning function as well as the staging of all equipment used in the construction of the new site. They also interface directly with County personnel at the proposed new site locations.

The structure of the new site installation service requires involvement from the County's General Services organization in those cases where the decision is made to have the structured cabling and other components installed by the County's selected vendor. All new sites do require the County to provide certain components—such as power and air conditioning—that are determined on a project-by-project basis.

- Methodology & Key Processes – Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's project management team uses standard Project Management Institute (PMI)-based Project Management Methodologies and has successfully used them to bring 87 new sites online for the County. These processes have been tailored to identify all site-specific activities needed to activate IT services at a new location. Contractor's project managers (PMs) actively walk the proposed site with County stakeholders and engineering

resources initially and at various points as the project requires. After requirements and the design are fully understood, the project plan, schedule, and task list are developed by project managers —laying out the details of the project as well as capturing internal and external dependencies. Identified as early as possible, dependencies under control of the County or County contractor are managed with a clear understanding of the associated impacts so that they do not become roadblocks to the project's successful completion. At project close, key learnings are identified and documented by the PM for sharing, learning, and continual improvement by the team.

Although external dependencies are not within Contractor's control, Contractor's team routinely focuses on these actions early in each project to mitigate the risk to completion of Contractor's deliverables. An example of this was the Health and Human Services Agency's move into their new Escondido facility. At a critical point in the project, difficulties in obtaining permits from the City of Escondido were identified. The AT&T team noted that these permits were a key dependency in the installation of telecommunications services to the site. To keep the project on schedule AT&T was able to leverage contacts within the City to obtain the necessary paperwork. Working in parallel, the AT&T PM also escalated internally so that AT&T leveraged resources were able to accommodate last-minute schedule changes and so that the County build and move-in schedule was maintained. For this effort, the product team was given the IT Customer Service Award by the County Technology Office.

Another aspect of Contractor's processes include how project RU billing estimates and final billing are determined as follows:

- Project Start: The network design and pricing estimates documented in the initial Scope of Work are based on the County-provided estimate of End-User occupants for the site.
- Project Completion: Upon project completion Contractor shall update the final End-User count in the SOW and present that to the County for project completion sign-off and billing initiation.
- Post Project 6 Months: Contractor shall perform a final true-up assessment 6 months from the County SOW sign-off. If the site End-User count has exceeded the tier limits for the new site RU originally bills, then Contractor shall initiate a billing adjustment.

5.17. Interactive Voice Services

Solution to meet the requirements

Interactive Voice Services are defined as an IVS system which builds on the basic services provided in Voice Services, includes one or more of the following capabilities:

- Call Management Reporting
- Call Recording
- Speech Recognition Application
- County data integration (data dip)
- Wallboard (Physical/Virtual)
- Computer-Telephony Interface (screen pop)
- Work Force Optimization
- Outbound/Predictive Dialer
- Agent Softphone
- Speech Enabled Customer Surveys

Three categories of IVS shall be created. Each shall provide for technical design, infrastructure, licensing, hardware/software maintenance and support and initial End-User training. The categories shall contain the following components:

- **Small IVS** – *shall include Automated Call Distribution (ACD) and/or Auto Attendant (AA) & Call Management System*
    - Automated Call Distribution (ACD)
        - Distributes calls to customer facing agents.
        - Supports the total contact center agent population at all County network locations.
        - Includes trunking infrastructure to support the routing of calls.
        - Can be used as a stand-alone component or in conjunction with an Auto Attendant.
    - Auto Attendant (AA)
        - Supports Touch-tone input to route calls across the County voice network.
        - Includes the professional recordings both English and Spanish menus and prompts.
        - Includes trunking infrastructure to support the routing of calls
        - Can be used as a stand-alone component or in conjunction with an ACD.
    - Call Management System (CMS)
        - Provides reports of contact center agent metrics such as abandoned calls, average talk time etc.
        - Used in conjunction with an ACD to manage contact center performance.
        - CMS is the additive feature which initiates the Small IVS RU category vs. the right-to-use ACD and/or AA capability associated with the Voice RU's.
- **Medium IVS** – *shall include all components from the Small IVS RU category and shall also include:*
    - Automated Call Recording (ACR)
        - Provides for up to 90 days of customer agent recorded calls for both compliance and quality purposes.
    - Virtual Wallboards
        - Provides ACD statistics and messages displayed on contact center agent and supervisor desktops.
    - Agent Softphone
        - Provides IP softphone via a desktop client that provides County contact center agents full functionality whether they are working at their primary County facility, a remote/alternate County site or at home.
- **Large IVS** – *shall include all components from the Small and Medium IVS RU categories and shall also include:*
    - Interactive Voice Response (IVR)

        - Platform for custom applications such as outbound predictive dialing, multi-language support, voice recognition and County data integration.
- Computer-Telephony Interface
    - Customizable interface between IVR and Desktop components to provide database information to a contact center agent when receiving a call from a constituent.
- Short Message Service (SMS)
    - Provides up to 200,000 outbound text messages to specifically defined County client lists.
    - Requires the manual upload of a County file of customer contact information to the hosted platform.
- Work Force Management
    - Centralized platform of work force scheduling, forecasting and adherence of contact center agents.
    - Provides long term strategic forecasting of agent resource requirements based on historical data
    - Integrated with CMS for agent call statistics
- Physical Wallboards
    - Provides ACD statistics and messages displayed on physical monitors in County call centers
    - Includes the controller infrastructure and supporting software to County provided monitors

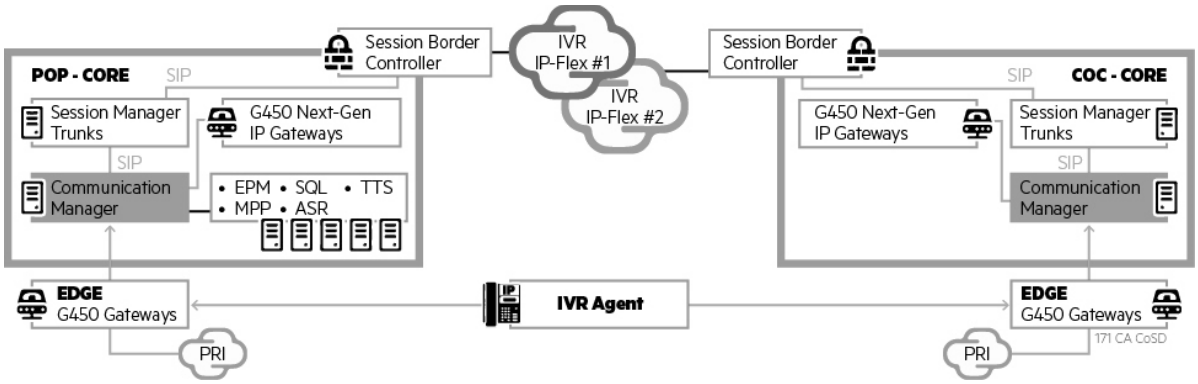
Integrated Voice Response

At the core of the functionality provided under IVS Services is the Integrated Voice Response platform. The IVR infrastructure is built around the Avaya Experience Portal, located at the AT&T POP. This platform provides IVR, self-service, touch-tone as well as speech recognition services for key contact center solutions across the County such as the Department of Animal Services, the Land Use Environmental Group, and various departments within the Health Human Services Agency. This scalable, high-availability infrastructure provides many options for programming and agent integration—allowing customization for any type of constituent-facing contact center service.

The platform shall undergo near-term changes relative to external telephony connectivity as AT&T initiates plans to implement dedicated, fault-tolerant inbound and outbound IP Flex SIP trunks for the County's IVR infrastructure at the AT&T POP and County Operation Center. This IVR solution shall not impact enterprise voice traffic, allowing business units to conduct high-volume contact center activities, such as outbound dialing campaigns. This new capability shall provide standardized resource unit base from which business units can leverage the platform. This upgrade shall be provided as a Transformation initiative and shall be included in Voice Services as a means to meet relevant scope requirements. Further details of AT&T planned transformation of IVR services is defined in Sections above, Transformation Services, subsection "Initiatives: Voice Services Transformation."

Over the term of the Agreement, Contractor shall ensure that AT&T develops a transformative roadmap, where proposals shall be developed to increase the redundancy and resiliency of IVR applications, as well as to provide additional feature benefits, such as automated agent call-back and web chat. The figure below presents Avaya's Experience Portal connectivity.

Avaya's Experience Portal Connectivity



Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.

- Resource and Facility

The County Operations Center and AT&T POP shall be the primary facility locations for IVS services. Over the life of the term, Contractor shall implement geo redundant systems for key functionality as well as make proposals to introduce new features and functionality. Refresh shall be performed for the systems on a five-year basis.

- Methodology & Key Processes – Key methodologies and processes for year-to-year continuous improvement

As mentioned above, the process for changes and enhancements needs reflect the County's need for flexibility. For minor/basic changes to existing voice applications, County may make these types of changes at no additional cost.

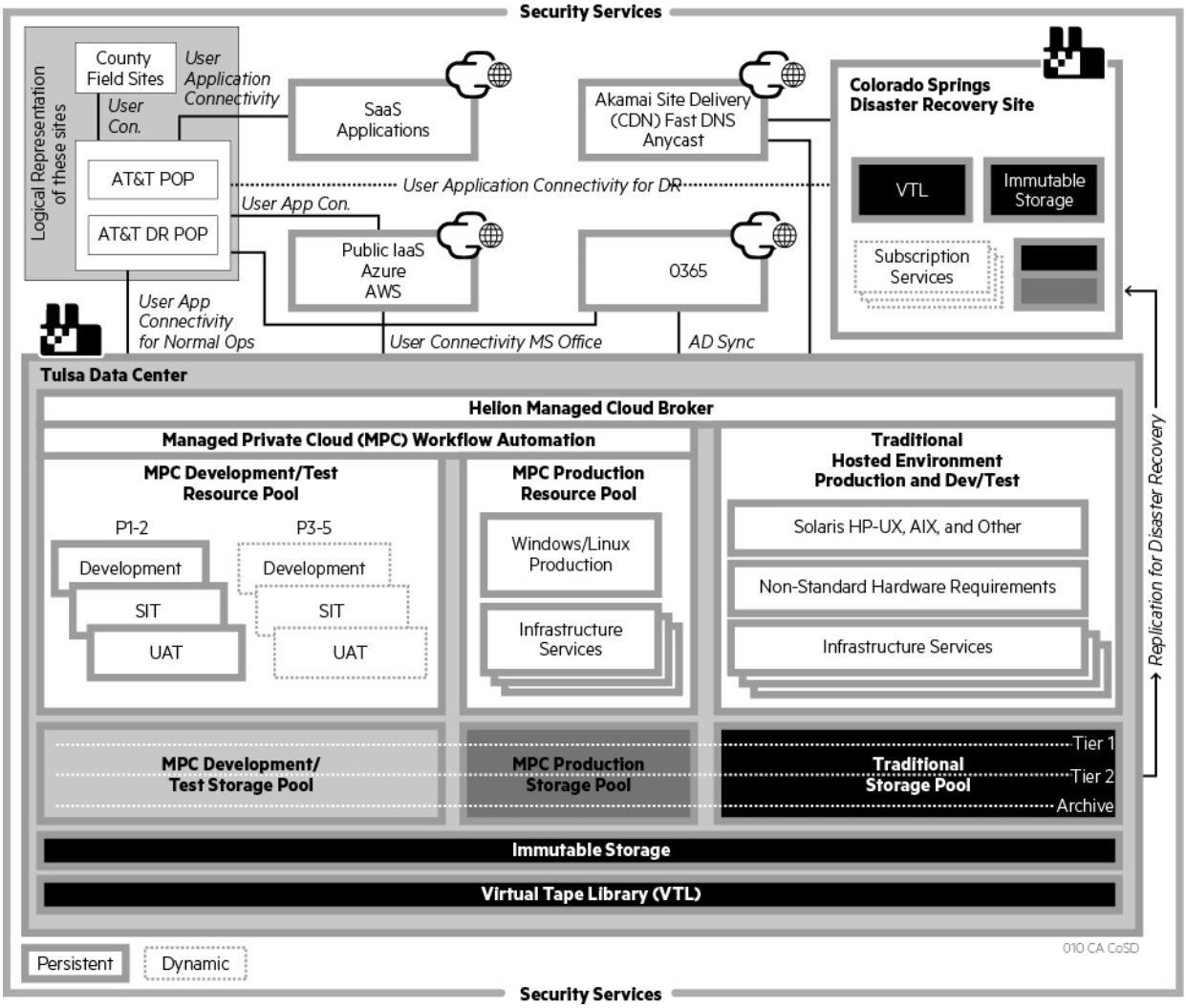
- Additions, changes or deletions to existing call flow/menu prompts
- Additions, changes or deletions to existing routing or transfer points
- Implementation of licenses associated with provided features
- Professional voice recording of changes on basic Auto Attendant and ACD systems

6. DATA CENTER SERVICES

6.1.1. Process and Procedures

Contractor shall provide a data center services framework solution, shown in the figure below, to fully meet the County's needs and facilitate consolidation of applications and infrastructure services into a single Tier 3 production data center in Tulsa, OK. This facility shall be ISO 9001:2008 certified and meet stringent public sector compliance and security requirements.

Contractor data center Services Framework Solution



Data Center location and solution as it relates to disaster recovery requirements.

The Contractor's Continuity Services center in Colorado Springs, Colorado, shall be the designated disaster recovery (DR) site for the County. Contractor's solution shall incorporate 100% redundancy of infrastructure, provided on a subscription basis, for applications that currently require a DR solution. Production data shall be replicated from Tulsa to the DR site using a dedicated network connection. Contractor's Colorado Springs center shall be a purpose-built, SSAE16-audited data center. The Tier III design shall provide a concurrently

maintainable and continually operating facility with infrastructure built with redundant capacity components and multiple independent distribution paths serving the computer equipment.

Contractor's solution shall meet required recovery time objectives (RTOs) of 48 and 72 hours while also eliminating the current dual data center architecture. The Colorado Springs DR site shall have sufficient capacity to support a dedicated environment for an active/active architecture, should the County decide to reinstate it. Contractor shall include in the solution the core network components (Akamai and Global Traffic Management capabilities) to support an active/active architecture.

The DR location and solution shall provide recovery of production midrange and private cloud environments as well as technical assistance for recovery of business processes. In case of a disaster, the production environment shall recover gracefully in Contractor's Colorado Springs data center.

Note that traditional VMWare and MPC environments are handled identically for DR purposes; the Managed Private Cloud is a collection of virtual servers, some of which have DR recovery time objectives, some which do not. The DR environments for the virtuals within the MPC shall be virtual servers that spin up with a copy of the MPC virtuals, for those servers that have designated RTOs in Apps Manager. The Colorado Springs DR site shall have the following features:

- It exceeds Tier 3 data center specifications and:
  - Is on two different power girds
  - Has multiple points of entry for telecom and Internet access
  - Has multiple on-premise power generators that are physically separated—in different rooms with fireproof walls—to make sure that, if there is a fire, Contractor does not lose all of Contractor's generators.
- Colorado Springs provides subscription offerings and Continuity professionals who are trained and certified in Business Continuity disciplines. They shall advance the County's Disaster Recovery strategy and testing methodologies to provide full assurance of application recovery that meets the County's requirements.

Contractor's Rancho Bernardo environment shall use replicated backup sets at the DR site in Colorado Springs to meet remote backup set storage requirements.

Identify and eliminate single point failures with infrastructure and portfolio applications in Data Center Services.

Contractor shall assess redundancy as part of Contractor's design process to avoid single points of failure in the infrastructure and for high-availability (HA) P-1 and P-2 portfolio applications, taking into consideration the criticality of the application or infrastructure element. Contractor shall build quality into the design process by conducting peer reviews so that changes or additions do not create single points of failure.

Contractor shall provide redundant switches in the data center and redundant circuits to the data center. The physical servers shall have redundant connections to the network and to the storage fabric. Physical servers shall be configured with redundant components such as redundant power supplies, which shall be plugged into separate power leads in server racks. Storage arrays shall have redundant components as well, such as redundant disks and power supplies, and shall have the ability to automatically notify Contractor's support teams when an alert is detected on the array. At the application layer, for business-critical applications, Contractor shall incorporate redundant web servers and application servers that are load balanced on the F5s. Databases for business-critical applications shall have replication and/or clustering enabled.

For those applications hosted in the cloud, the Helion Managed Private Cloud (MPC) shall incorporate the tools necessary to continuously monitor server availability across the environment to maintain hardware, upgrade firmware, investigate outages, and perform corrective actions to restore hardware when necessary. Both the MPC and traditional VMware environments shall include spare physical servers that can take over the virtual server load in the event of loss of a physical server in the virtual farm.

The MPC hybrid cloud eliminates single points of failure and meets the service level (SL ID 51) for application availability.

For applications that are unable to meet Service Level 51 without additional redundancy (in both the MPC and traditional environments), Contractor shall add the necessary redundant components upon approval by the County.

The Data Center Services solution for the County shall incorporate the following:

- **Facility Redundancy**: All key components shall be concurrently maintainable, as defined by the Uptime Institute for Tier III facilities, including N+1 data links, power, uninterruptible power supplies (UPS), and cooling as well as redundant network connectivity, power supply, and electrical.
- **IT Architecture Redundancy:** The MPC architecture shall be able to host enterprise-grade workloads that demand high levels of system availability and performance in x86 private clouds. Contractor shall maintain a "system-level" service level objective (SLO) up to 99.95% availability for the entire Infrastructure as a Service (IaaS) stack. This shall include maintaining the availability of the compute; storage; network; security; backup hardware and software, up to and including the operating system (OS); the Cloud Service Automation (CSA) software; and Contractor facilities.

To eliminate server failures, the majority of County traditional hosted applications shall run on VMware virtual machines (VMs). VMware HA shall automatically move and restart VMs on other VMware host servers in the County cluster in case of failure or planned maintenance.

Applications that run in a Solaris operating environment shall use server clustering technology to provide redundancy when needed. Oracle servers requiring high availability shall be deployed in server clusters. If the primary server node fails, services shall automatically fail over to the redundant node. Failover shall also be able to be invoked manually to support a planned outage. More specifically, Contractor shall provide redundancy to the Solaris environment in the following manner:

- Disk
    - OS disk (internal disk): primary/mirror/altboot on three separated disks
    - Application files (external disk array): hardware redundancy
- HBA: At least two host bus adapters (HBAs) per server using either MPXIO or Veritas DMP for multi-pathing
- Networking: At least two physical interfaces for production IP using IP network multi-pathing (IPMP) or link aggregation.
- Server hardware: at least 2 power supplies/ two CPU cores

Private cloud and traditional hosted storage shall use HPE 3PAR enterprise storage designed for cloud environments. The storage shall host OS images, virtual snapshots, and application data. All OS images for virtual machines shall boot from the storage area network (SAN). This architecture shall enable the server image to be disassociated from the physical hardware, allowing the server image to move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover for improved availability.

- **Application High Availability**: Contractor shall use the F5 BIG-IP Local Traffic Managers (LTMs) to provide the County application HA by load balancing applications across multiple VMs.

  Contractor shall maintain and support, database clustering tools such as Oracle RAC (e.g., for Oracle IDAM) and SQL Always-On (e.g., for SharePoint 2013) where in use or planned to be in use. The cost of such licenses for database clustering is not included in base services.

- **Disaster Recovery**: To cover higher requirements for redundancy to handle RTO/RPO requirements on mission-critical applications that include P1 Apps – 48 hours with <= 28 hours of data loss and P2 Apps – 72

hours with <= 28 hours of data loss, and services during a declared disaster event, Contractor shall integrate Contractor's Helion Continuity Services delivered through the Colorado Springs DR site.

- **Server Management and Monitoring**: Contractor shall install, manage, and monitor the OS instance and the underlying virtual and physical server. Contractor shall monitor server availability, maintain hardware, upgrade firmware, investigate outages, and perform corrective action to restore hardware when necessary. Contractor shall also maintain the health of infrastructure assets included in the solution, including server, storage, backup, network, and other devices. Contractor shall use HPE Operations Manager (HPOM) and SiteScope to detect problems and send selected alerts to a centralized management server for specific business-critical applications for County business groups. Thresholds shall be set on events to indicate potential problems, so that support teams can respond to them in time to prevent outage incidents.
- **Special Scenarios: Multi-Facility Presence (active/active facility-level requirements).** In the single data center model, the redundancy components described in the "IT Architecture Redundancy" bullet above shall be applied to applications to provide high availability. For example, the Netmotion environment consists of a single application server and a single database server in each data center. Following the consolidation to Tulsa, this configuration shall be replaced with two load-balanced application servers and two clustered database servers. This provides automated failover within the Tulsa site – a more robust configuration than the manual failover configuration in place today.

If the County wishes to return to a multiple-primary data center model for specific applications, Contractor can locate specific servers at other sites. The location and cost of this approach shall depend on the volume and design required.

Design and support an all virtual infrastructure in the data center.

Contractor shall provide virtualization on a standardized platform to further reduce the number of servers needed.

Approach to Design and Support an All-Virtual Infrastructure: The MPC implementation for the County shall serve as the platform to support an all-virtual environment, providing the bridge from a hybrid environment to an all-virtual environment when feasible. Contractor shall initially retain existing applications in the traditional hosted environment until scheduled for refresh or application upgrade. At that time, Contractor shall collaborate with the County, performing a cost/benefit analysis to determine feasibility to migrate additional applications to the MPC environment. In this analysis, Contractor shall take into consideration items such as level of County hardware investment, timeframe for application retirement, if any, and the level of effort for legacy applications to be re-architected to run in the MPC, if applicable.

MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases. Contractor as part of the solution design shall incorporate the license considerations to manage costs with the expectation of no change in license costs increase based on the virtual solutions.

As part of the Data Center Consolidation transition design process, Contractor shall make all reasonable efforts to optimize County software licensing costs. County software has a variety of licensing models such as site/enterprise, concurrent user, named user, module, managed budget, server, CPU, and core. Licenses based on server, CPU, and core present an opportunity for consolidation and license cost savings.

Methodologies to reduce license obligations for server/CPU/core based licenses shall include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated to headroom at each site versus single site's shared environment. Contractor shall pursue these methodologies during the design phase of the Data Center Consolidation.

Contractor shall leverage virtualization at the server, storage, and network levels. Virtualization shall separate the applications, data, and network connections from the underlying hardware. Through storage virtualization, the

County shall be able to increase utilization ratios and have greater data tiering flexibility to right-size storage and performance to meet application-specific requirements. With HPE virtualized SDN switches, network provisioning shall be streamlined, making it easier for Contractor to monitor connections.

Contractor shall be familiar with external requirements, such as State or Federal mandates, that can affect the underlying technology demands. Contractor shall collaborate with the County to establish thresholds and project application workloads. Contractor shall combine this information with infrastructure utilization data to create tactical and strategic capacity plans to verify that the County's environment in Tulsa shall accommodate growing and changing business requirements without jeopardizing performance standards.

The MPC infrastructure shall provide the capability to expand capacity quickly due to unforeseen circumstances or emergency situations. This infrastructure shall be supported by Contractor data center professionals who understand the County's business and technical needs. Contractor shall use Contractor's industry-standard software tools to monitor and measure storage capacities and server central processing unit (CPU), memory, disk, and input/output (I/O) utilization and performance on a daily basis.

Contractor shall analyze daily and monthly capacity reporting to identify and address day-to-day capacity constraints. Additionally, Contractor shall analyze capacity trending reports to identify recurring problems that require system upgrades or system refreshes. Contractor shall continue to assess the impact of all changes on the capacity plan and the performance and capacity of all services and resources; tune and optimize the performance; implement County-defined policies; and develop methods to effectively monitor, measure, and report on capacity across the environment. Contractor shall also work with the County departments as they capture forecast demand to produce and maintain a quarterly Capacity Plan that defines planned server system upgrades and refreshes based on growth of existing as well as new application workload. The team shall update the existing capacity plan to reflect each year's forecast. Capacity planning for the County shall encompass the following:

- **Servers** – Capacity management services for servers and mainframes and associated storage shall include monitoring system usage and capacity by analyzing historical resource trends. Contractor shall apply this data during decision-making reviews to assist in formulating environment requirements that meet or exceed future business requirements. Contractor's comprehensive suite of server management and monitoring tools shall monitor the servers against thresholds and alert operations when there is an issue. Metrics shall be captured and run through a data warehouse for trend analysis and capacity planning. Monitoring metrics shall be summarized each day and reported.
- **Planning for Increased Application Usage** – Contractor shall enable performance analysis and availability management to allocate capacity dynamically. Contractor shall use system metrics and statistical reports to gain a clear understanding of overall capacity trends and performance. Contractor and the County shall use this information during decision-making reviews to reshape the compute environment periodically.
- **Network Capacity Planning** – Contractor shall continue to monitor data network usage and performance and generate capacity reports that identify actual and potential network bottlenecks, by establishing capacity benchmarks and by analyzing trends. Such trends shall address the form of overall throughput, percent usage, error rates, and specific performance metrics such as packets per second. Contractor's metrics shall measure both peak and average performance. Contractor shall offer network capacity recommendations for tuning the network to improve efficiency and cost effectiveness.
- **Storage Capacity Planning** – Contractor's storage infrastructure shall support the ability to expand capacity quickly due to unforeseen circumstances or emergency situations. Contractor shall use Contractor's industry-standard software tools to monitor and measure storage capacities, disk, and I/O utilization and performance on a daily basis.

Hyper-converged infrastructure in the delivery of virtual infrastructure.

Contractor shall provide Helion MPC and Helion Managed Cloud Broker (HMCB) to be implemented during the transition period as Contractor builds the County's on-demand Dev/Test and production environment as part of

the data center consolidation. By implementing a private cloud with standard-sized building blocks of virtual infrastructure, Contractor shall be able to analyze whether hyperconverged infrastructure shall ultimately yield benefits for the County. If Contractor is able to fully standardize over time on the x86 platform in the converged infrastructure, then the next logical step would be to move to hyperconverged infrastructure as the data center components come up for refresh. When the County is ready for hyperconvergence, Contractor stands ready to be the County's technology partner to accomplish this objective.

Hybrid cloud integration with data center.

Contractor's in-depth knowledge of the County environment and business objectives enables Contractor to design a hybrid infrastructure strategy that most effectively applies to the County's portfolio of services, accommodates the required workloads, and enables desired business outcomes. Contractor's hybrid approach to enterprise computing combines traditional IT resources for some applications—such as Solaris, HP-UX, AIX, and others—while Windows and Linux applications can be deployed in the cloud. The Contractor's hybrid solution for the County incorporates MPC services with traditionally hosted applications in the Tulsa data center, as described in Application Infrastructure Services.

The HMCB layer enables the County to see all resources —traditional, private cloud, and, in the future (if desired), public cloud such as Amazon Web Services (AWS) and Microsoft Azure—as a unified infrastructure. HMCB shall provide a centralized management layer for traditional and cloud resources managed by Contractor. Contractor's design and architecture shall provide interoperability and integration of tools and common resources (such as storage, network, and security components) with the applications that remain in a traditional hosting environment, enabling smooth transition to hybrid IT.

Contractor shall provide a hybrid model, built using the MPC, customized to the County's requirements, that is scalable and works with the County's infrastructure. Contractor shall optimize the County's applications, as described in the Methodologies and Key Processes section of Application Infrastructure Services to identify which applications are to be in the MPC and which Contractor recommends remain as traditionally hosted.

Additionally, upon integrating hybrid cloud, Contractor shall consider open standards that avoid vendor lock-in as well as architectures with the flexibility to meet the County's changing needs. Contractor shall address the following:

- Continue to support and integrate with the workloads that currently run the business
- Integration must bridge the current applications and workloads with those planned for the future
- Applications differ in how they are designed, hosted, and consumed
- Applications have different infrastructure requirements

Contractor shall use a single management toolset, described in Application Infrastructure, to manage different types of resources. Policy-based placement makes certain Contractor shall deploy workloads to the right infrastructure based on specific business requirements.

Process for physical and virtual servers.

Contractor's hybrid solution shall include Helion MPC services combined with traditional hosted services.

MPC Provisioning: Implementation of HPE's Helion MPC shall enable Contractor to quickly deploy new services where virtual infrastructure is automatically provisioned in hours or less instead of days, upon approval from the County. To provision virtual servers, upon approval by the County, Contractor shall finalize the approved Solution Design Document (SDD) or Confirmation of Server Requirements and shall perform the following tasks for MPC server provisioning:

- **Access the MPC Provisioning Tool** – This provides an intuitive graphical user interface that Contractor shall use to select from a prepopulated catalog of services that Contractor shall define during the MPC build, including provisioning of virtual servers.
- **Browse the Service Catalog** – Using the catalog, Contractor shall browse all predefined offerings and select the primary service desired to initiate the provisioning process.
- **Configure the Requested Service(s)** – Once Contractor has selected a primary service to reflect approved County requirements, the associated selectable options shall be available to Contractor's MPC provisioning team. For provisioning virtual servers, Contractor shall choose the County's required minimum SL, the server name and size including quantity of CPU, RAM, and primary disk size, network connections, server OS, and target resource pool (applications infrastructure, infrastructure, or Dev/Test). Contractor shall then select from a list of predefined templates, which are the County's gold images. Next Contractor shall choose to add-on optional services such as predefined backup and storage choices as required to meet the County's specific workload requirements. Contractor shall then add the item to the cart and repeat this process as needed to configure multiple approved servers simultaneously prior to checkout. Note: Contractor can also reorder or place a request to initiate new services based on prior requests; this streamlines the process.
- **Place the Order** – When the configuration is complete, Contractor shall review and confirm the requested items and confirm the new service(s) or modifications to existing services.
- **Order Fulfillment** – The Contractor initiator receives notification when the automated order fulfillment process is launched, and continues to receive status notifications until provisioning is complete. Contractor shall notify the County once the services or changes are ready.
- **Manage Service Orders** – Notifications shall enable Contractor to track order status in real time. Contractor can also access, monitor, and perform actions on services (such as modifications, cancellations, or deletions), view a detailed list of all orders, and approve requests. Once a service is marked for deletion, a 7-day retention policy is enacted to safeguard the data in case this process needs to be reversed if requested by the County. Additionally, Contractor can track status of servers such as Online, Offline, Transitioning, Reserved, Deploying, Modifying, Modification Failed, Failed, Canceling, Cancellation Failed, Expiring, and Expiration Failed.
- **Manage Services –** For services currently subscribed and running, Contractor can view detailed information about the services and topology as well as the individual components that constitute the overall service delivery. Within this view, Contractor can also request actions such as start, stop, reboot, create or revert snapshot, server resize, and more to manage the County workloads in an expedited manner.

MPC provisioning shall be powered by the following underlying technology and processes:

- **Cloud Service Automation (CSA)** – Combined with Operations Orchestration (OO) and Matrix Operating Environment, CSA automatically enables the design and provisioning of virtual infrastructure services in hours instead of days. HPE Server Automation software shall enable Contractor to automatically perform activities such as server discovery, provisioning, patching, configuration management, and script execution to comply with IT configuration standards.
- **Computing Services** – Contractor shall preconfigure the image for automated provisioning. Using administrator privileges, Contractor shall provide OS patching and ongoing maintenance as well as all database and application installations, patching, and ongoing maintenance. Contractor shall monitor system availability and security, and perform root-cause analysis and corrective action of OS; physical and virtual servers; storage, backup and network environment problems; and all other IT Service Management functions.
- **Storage Services –** Contractor's Helion Storage Services enable efficient information management while maintaining the right level of storage from creation to deletion. Contractor shall manage the County's active system data via a storage area network (SAN) platform using tiering technologies to balance cost and performance; this delivers a lower-cost solution, increases business agility, and minimizes risk. Contractor shall virtualize storage resources to increase utilization and provide greater data tiering flexibility.

Contractor shall provision storage infrastructure (hardware, software, and management tools) to store application and database data from the corresponding computing environment. Features include storage performance and capacity planning, monitoring, reporting, asset management, service operations management, and supplier engagement, when necessary.

- **Server Provisioning, Monitoring, and Management** – Contractor shall install this service and configure it to meet County-specific needs based on the following:
  - Resource pool location for capacity provisioning
  - Availability "System Level" end-to-end Service Level for availability
  - Server size (CPU configuration: x-small, small, medium, large, x-large)
  - Server size (GB of RAM: x-small, small, medium, large, x-large)
- **OS Provisioning, Monitoring, and Management** – Contractor shall install a standard build for the Windows and Linux operating systems and monitor availability of the servers and the OS instances up to the point of connection with network demarcation. Upon detection of an availability, capacity, or performance event, Contractor shall investigate the outage and perform corrective action to restore the system. Contractor shall deploy local admin users for Contractor's Private Cloud Operations OS administration. Contractor's OS management shall include startup and shutdown, OS patch management, and maintenance job scheduling (at the OS and system level) for private cloud internal management activities.
- **Policy-driven Automated System Provisioning –** Contractor shall automatically provision new cloud infrastructure based on defined policies. New systems are deployed once approved by the County, and Contractor shall periodically advise the County when new OS versions and editions become available.

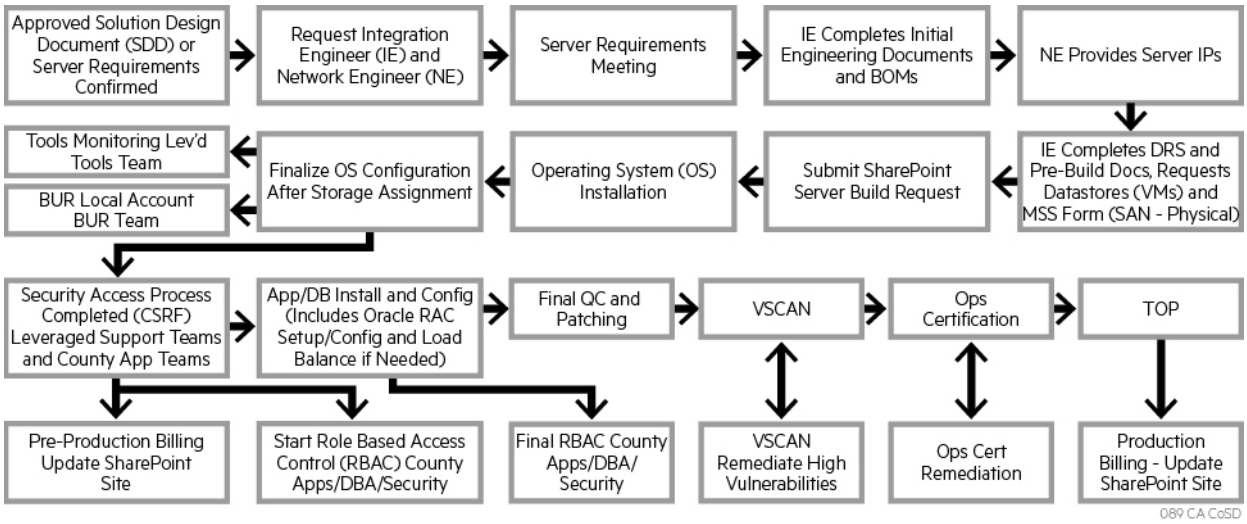
Traditional Provisioning: Using HMCB, Contractor shall perform automated provisioning of VMware servers in the traditional environment. Over the long term, Contractor recommends that all VMware environments within the data center be moved into the MPC and the HMCB provisioning process be used for non-data center servers. The provisioning process for VMware servers in the traditional environment follows the steps above up to the point of layered product installation, at which point Contractor follows the traditional process, described below.

Contractor shall have an established and thoroughly documented process to provision traditional servers that begins when the Contractor server team receives an approved Solution Design Document (SDD) or Confirmation of Server Requirements from the County.

This process shall incorporate all the necessary engineering activities and includes installing the OS, configuring the necessary storage capacity, applying security controls, scanning for vulnerabilities, testing, deployment into the production environment, and finally provided appropriate access to the Applications team to start development or testing as needed.

Adherence to this process shall enable Contractor to meet the County's Provisioning Service Levels.

Contractor Standard (Traditional) Server Provisioning Process



Physical Server Provisioning shall follow the same process as Traditional Server Provisioning, with the following steps added, following the approval of the SDD:

Workload Placement is a step that engages the Hardware Planning team to determine the floor and rack locations and provide any additional power and cabling, if required.

Network Configuration: Switches and remote access capability are configured.

Hardware Installation: If sufficient hardware is available within the pool of spares, this hardware shall be integrated and installed and connected, once the floor and rack locations are ready.

Procurement shall occur to replenish any spares used by the request; or, for large or specialty hardware orders, this step shall occur before hardware installation.

Storage Configuration: SAN fiber shall be connected and LUN allocations shall be presented to the physical server.

6.5. Security Services

6.5.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall consolidate all services (except mainframe and AS400) from Plano, TX and Tulsa, OK (Tulsa) into a single production data center in Tulsa. The new environment shall incorporate a Managed Private Cloud (MPC) environment for production (upon county approval), development/test (Dev/Test) services, and Break/Fix, and retain the traditional hosting infrastructure for production, Dev/Test and/or Break/Fix that are not compatible. It shall include the deployment of firewalls, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

devices, host-based security and full spectrum analysis of all traffic in and out of the Tulsa data center. Contractor shall incorporate robust IT security within the Tulsa data center to meet the specified requirements. Contractor's approach to data center security shall involve disrupting the entire life cycle of an attack, by investing in both layered prevention and detection, and in a network configuration that creates separate security zones.

The Contractor solution shall include:

- **Implementation of Palo Alto next generation firewalls.** These multifunction devices provide firewall services, intrusion prevention and detection services, spyware and antivirus filtering, web content filtering as well as unified threat management capabilities. This solution also provides automated alerting of possible malicious activity and daily threat updates.
- **Network zone restructuring.** The production zones shall be implemented by a combination of network segmentation, device separation, and firewall separation between each of the three zones (Front DMZ, isolation zone, and data center zone). The Dev/Test environment has virtual local area networks (VLANs) representing each of the three zones. The Dev/Test environment shall mimic the production environment. That is, VLANs for Dev/Test shall be located in each of the zones (front DMZ, data center zone and isolation zone). The Dev/Test VLANs shall be segregated from the production VLANs by the firewall and shall not have access to the production VLANs, unless access to specific Services are required (e.g. Active Directory). If a firewall change is required by M&O activity, all labor associated to the firewall change shall be covered under Apps M&O. If the firewall change is required by a new application, it shall be included as part of the project. In addition to eliminating the security risk, it shall provide for more comprehensive application testing. Applications shall be able to test firewall rules earlier in the process and hone during testing. This shall facilitate a cleaner cutover to production.
- **Expansion of ArcSight Security Information and Event Management (SIEM) Services.** All firewalls and IPS sensors, VPN devices, and DHCP appliances in San Diego, Plano, and Tulsa shall be enrolled in SIEM services (log collection, log management, and reporting as well as 24x7 alerting and monitoring services). In addition, Contractor shall include "critical servers" such as domain controllers or servers with data subject to regulatory compliance, such as HIPAA and PCI.
- **Email Security.** With the transition of email to the cloud, email-specific security services shall be provided by the Exchange Online Protection (EOP) capability, which provides comparable security services to the IronPort appliances, such as:
  - Data Loss Prevention (DLP) for email
  - Advanced Threat Protection (ATP)
  - Exchange Online Archiving for Exchange Online
  - Legal Hold
  - Antispam/Antimalware at the mailbox level

- **Distributed Denial of Service (DDOS).** DDOS protection shall include protection at the Internet Service Provider (ISP) layer outside of the County environment, firewall configurations, network configurations, Access Control Lists (ACLs), intrusion prevention system configurations, Web/DNS traffic DDOS protection provided by Akamai, endpoint protection on all windows systems, operating system hardening, browser protection as well as application level protections.
- **Active Directory.** The following components of AD2012 shall be re-engineered as part of the consolidation during transition:
  - Domain controller redundancy standards (rule of three) for the CO domain
  - Flexible single master operation (FSMO) roles failover locations for CO and County domains

- Contractor shall also implement the following tools:
  - **Dell Recovery Manager Active Directory (RMAD)**. RMAD functionality includes the restoration of deleted objects as well as corrupted objects and provides the ability to recover an entire domain or forest in the event either of these is lost or corrupted. RMAD eliminates the need to recreate impacted objects and results in quicker service restoration.

- **Dell Enterprise Reporter**. Enterprise Reporter provides reports related to Active Directory, which shall provide the County the ability to monitor and manage End-User access and respond to audits.

- Deployment plan for resources and use of facilities

Contractor shall support security services using a combination of resources dedicated to the County and Contractor leveraged resources with specific areas of expertise. These shall include the Contractor CISO, Contractor Security Operations Manager and leads for the various functional areas (threat management, access management, security engineering, risk management among others). The Contractor security teams shall provide the daily support of the various security services and security infrastructure components based on their area of expertise.

Contractor security staff shall be located at the following sites to support the County:

- Rancho Bernardo. Primary location of Contractor staff specifically assigned to support the County. Test environments, training, and video conferencing are housed at this site as well.
- Contractor's Tulsa Data Center – Tulsa, OK – This is the production data center that shall house the majority of the County IT infrastructure, except for that located in San Diego, and delivery of core IT and security services.
- Contractor's Colorado Springs Disaster Recovery (DR) site – Colorado Springs, CO – This location shall be the DR site for the County data center services. It shall provide back up or failover capability for all Tier 1 and Tier 2 applications, core services, and data center security services.
- Contractor's Orlando Data Center – Orlando, FL – This location hosts the SIEM services.

- Key methodologies and processes in solution including year-to-year continuous improvement

Security services for the data center shall be based on the defense-in-depth model developed by the National Security Agency (NSA).

The defense-in-depth model shall also tie to the controls specified in the Risk Management Framework (RMF). As controls are updated in the RMF roadmap, the defense-in-depth mechanisms and associated delivery processes shall be reviewed to identify any potential changes. The potential changes shall be reviewed with the County to determine implementation approach and timing and are added to the security operations roadmap. This roadmap shall contain items to further improve the security posture or maturity of the County from an operational perspective.

All Security hardware and software versions shall be evaluated upon release with consideration for feature benefit and risk. No deviation from standard shall occur without County approval. Patches and updates shall be evaluated as they are made available to determine their applicability to the County environment and shall be deployed immediately as needed.

For cloud based solutions, there are two scenarios for security integration:

1. For cloud services hosted by Contractor, Contractor shall provide end-to-end security implementation, testing, and continuous monitoring.

2. For cloud services not hosted by Contractor, Contractor shall provide, at a minimum, security implementation, testing, and continuous monitoring for all components under Contractor control, such as network and End-User devices.

Contractor shall follow a detailed Security Management Plan tailored to the County that defines the processes used to provide security services and roles and responsibilities for service delivery. It shall describe the technologies and interactions that comprise delivery of security services.

6.6. Mainframe Services

6.6.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide seamless, ongoing operational support to the SA16 LPAR Mainframe and A/S400 in Plano until migration to the new, web-based Integrated Property Tax System (IPTS).

During this time, Contractor shall:

- Be responsible for producing and submitting recommendations for standards on production jobs and Job Control Language (JCL)
- Develop and execute plans to retire the Mainframe and A/S400 upon approval from the County.
- Support Mainframe applications for migration
- Measure Mainframe usage in CPU hours and correlate CPU hours directly to End-User processing for specific applications
- Provide hardware and software utilities to support the Mainframe services
- Be responsible for licensing for all hardware and software used to provide Mainframe services.

As long as the mainframe and A/S400 are live in Plano, Contractor shall support the existing network connectivity that provides End User access, as well as the connectivity to Rancho Bernardo for Managed Print. The DR subscription for the mainframe shall be provided out of Contractor's DR site in Littleton, Massachusetts. Connectivity to Littleton for County End-Users is provided via T1

- Deployment plan for resources and use of facilities

The Contractor team located in Plano shall support the Mainframe until migration to IPTS (mid-range) is complete. Additionally, Contractor staff located in Rancho Bernardo shall support the applications. Following decommissioning of the mainframe, Contractor shall support the IPTS system in Tulsa.

- Key methodologies and in solution including year-to-year continuous improvement

Contractor shall use the following four-step process to decommission the SA16 LPAR Mainframe and AS/400 environments:

- Upon completion of the migration to new applications from the Mainframe and AS/400 environments, Contractor shall decommission the hardware according to standard change management procedures.
- As part of the hardware de-installation process, Contractor shall perform a complete wipe of the disk and tape storage to remove any County specific data. Contractor shall perform a data scrub of all hard drives, permanently removing sensitive data.
- All data stored on tape shall be evaluated for archive requirements. If data archive is required, Contractor shall convert the tape data for access by the new platform. All other data shall be removed (scratched) from the physical media, and either returned to the physical tape scratch pool, or destroyed depending on the condition of the physical media.
- Once the data removal process is complete, Contractor shall remove all hardware from WAN and LAN access. The DASD and tape hardware shall be returned to the Contractor leveraged storage pool for redeployment. The processor environment shall be de-installed and securely disposed.

Following the successful decommission of the mainframe and A/S400, all circuit connectivity to Plano and Littleton for the County shall be decommissioned, and the DR contract cancelled. Any tape media located at the DR site shall be recalled and handled as described in the third bullet above. Contractor shall evaluate the

connectivity required for the transmission of interface files, and, if necessary, shall continue to maintain the dedicated circuit.

6.7. Application Infrastructure Services

6.7.1. Process and Procedures

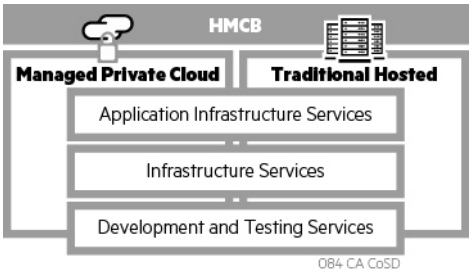
- Description of solution to meet the requirements

To maintain and support County portfolio applications, Contractor shall deploy hardware and software needed to sustain a hybrid computing solution that crosses three framework services, as illustrated in the figure below. Contractor's implementation shall include HPE Helion Managed Cloud Broker solution (HMCB) to provide a high level of automation and orchestration across two pillars: MPC and traditional hosted environments. With HMCB, Contractor shall have the ability to optimize and manage workloads across MPC, traditional hosted VMware, and, in the future (at the County's discretion) other cloud service providers by providing a full service management solution that gives Contractor a single view of the County's IT assets and governance across service management, financial management, operations, and analytics. For applications that are more complex and require greater customization, the traditional hosted environment shall enable Contractor to leverage the County's existing technology investments, and reduce risk by maintaining those environments until and unless they are ready to move. Within these two pillars of the design, each environment shall have its own resource pools for compute, storage, and network, providing the separation of resources required by the County. These resource pools shall be a logical separation. As previously noted, production applications shall not migrate into the MPC during Transition, but shall reside in the traditional VMWare environment until refresh, or such time as Contractor and the County wish to move them.

Contractor shall provide application infrastructure services from the Plano and Tulsa data centers. Contractor shall move compatible platforms in the current application infrastructure from a traditional hosted environment to a more agile MPC. MPC shall support approved versions in accordance to approved County technology standards of Windows and Linux virtual servers.

The pre-defined starting sizes for MPC servers shall be as follows:

Foundation for Application Infrastructure Services



SIZE	CPU ALLOCATION	RAM ALLOCATION
Extra Small	1	2
Small	2	4
Medium	4	8
Large	8	16
Extra Large	8	32

Note that this is only for resource allocation and is unrelated to the billing structure. This range of sizes covers most of the servers in the environment that have a compatible operating system. For servers whose resource requirements are higher (e.g., servers that require 64GB or more RAM), they can still be deployed in MPC as Extra Large, then the resources can be scaled up to meet the application's requirement. Fewer than 10 servers in the environment fall into this category; hence, Contractor did not design additional sizes. If, however, larger resource requirements become more prevalent, additional sizes can be added.

The hybrid environment shall support application infrastructure services, infrastructure services and Dev/Test services (for both Applications M&O and Development and Test projects). The MPC and the traditional hosted infrastructure are sized to accommodate the combined workloads from Plano and Tulsa, and can scale as needed to support the County's needs.

The approximate split of servers between the Traditional and MPC environments is as follows:

Development (Dev/Test + M&O Break/Fix)	271	60

In support of the County's Virtual First strategy, Contractor shall continue to pursue virtualization of as much of the remaining physical environment as possible. When each server comes up for refresh, Contractor shall analyze the rationale for keeping it on a physical server vs migrating to a virtual (and, if possible, migrating it into the cloud environment), and if there is no technical reason a physical server is required, Contractor shall redeploy the server's applications into a virtual server and dispose of the vacated hardware.

MPC Provisioning

As new applications are developed that are targeted to run in the MPC, the Contractor team shall request MPC resources through the provisioning interface, including servers, software, storage, and backup requirements. Once the demand request is received by the system, and the automated parts of the provisioning process complete, the Applications team shall then be responsible for installing, configuring, and testing each application component.

Conversely, as applications are retired or their Dev/Test components are no longer needed for live use, and therefore the associated MPC resources are no longer needed, the Applications team shall submit a service request to de-install the MPC infrastructure for that application. The team shall decommission all of the application components and infrastructure resources for the application environment being retired, and release any licenses through Asset and Configuration Management. If the environment is a Dev/Test environment, the request shall specify whether the environment is to be permanently decommissioned or put into cold storage. If the latter applies, the image shall be preserved on the storage area network (SAN) storage and held in an online inventory, but its compute resources released. Otherwise, all resources shall be released.

From a RU billing perspective, RUs are added to billing at the point a production server environment is made available for County use. RUs are removed from billing at the point when a request to decommission a production environment is issued and approved. If a production application moves from a traditional hosted environment to MPC (as shall be the case during Transition), the old RUs are removed and new ones take effect at the point when the MPC environment becomes available for County use. During Transition, the County shall not be billed for both sets of RUs for any given server. Any move post-Transition from legacy environment to new environment shall be provided at no additional cost to the County, provided that nothing in the legacy environment has changed in a manner that causes additional cost to Contractor.

After Transition is complete, moves between the traditional Dev/Test environment and MPC hosted Dev/Test environment shall not have an impact on billing. Changes to the overall scope of the Development & Test Environment RU shall follow the contract change control process.

For additions to the Dev/Test environment, if the application resource requirements are large, such that its requirements exceed the capacity available (this scenario shall be the exception rather than the rule), Contractor may need to acquire more resources and modify Resource Unit fee accordingly. In most cases, the resources shall be available, and the environments shall be added with no change to RU billing. By the same token, removal of applications from the Dev/Test pool shall not trigger a change to RU billing.

For a description of how Contractor shall manage RU billing during Transition, please refer to, Transition Services.

Managed Private Cloud Specifications

The HPE Helion Managed Private Cloud solution shall be built on a predefined, dedicated solution that enables Contractor to rapidly deploy server, storage, and network infrastructure "as service" for the County via a secure, web-based Private Cloud Portal.

The comprehensive private cloud solution shall include HPE hardware and software, professional consulting and implementation services, and ongoing end-to-end management services. The foundation for the solution shall be HPE CloudSystem Foundation. HPE CloudSystem Foundation is a pre-integrated solution that shall enable Contractor to create and manage virtual pools of servers, storage, backup, and networking resources on behalf of the County using a common management layer.

Helion MPC solutions shall leverage CloudSystem Foundation to provide a predefined, prebuilt, highly standardized infrastructure environment. The configurable infrastructure environment shall consist of a set of preconfigured, dedicated hardware building blocks for computing, storage, backup, and connectivity. These building blocks—which can be scaled independently—shall serve as the underlying, enabling infrastructure used to provide the standard Infrastructure-as-a-Service (IaaS). There shall be a base service to which optional services, or building blocks, can be added. Using this approach, Contractor provides an MPC solution that shall be configured to the County requirements, including selection of the mix of virtual machine (VM) sizes and operating system distribution that best map to the County's application profile.

Standard hardware-related services supporting the private cloud environment shall include but not be limited to the following:

- Hardware installation and configuration
- Hardware management
- Capacity management
- Problem monitoring, including proactive hardware support
- Release management
- Patch and system driver management
- Data center facility (floor space, power supply, cooling, wiring)
- Installation of management software

Some of the standard hardware and software products shall be as follows:

- **Server, Storage, and Backup Devices** – MPC uses HPE's Converged Infrastructure including ProLiant Gen9 blades running inside c7000 blade enclosures. Integration with SAN-based storage and backup devices is required in support of an MPC environment. Contractor's private cloud offering uses 3PAR storage options as a configuration standard.
- **Cloud Service Automation (CSA)** – Combined with Operations Orchestration (OO), CSA automatically enables the design and provisioning of infrastructure services in minutes along the End-User-requested

infrastructure configuration. HPE Server Automation software enables Contractor to automatically perform activities such as server discovery to provisioning, patching, configuration management, and script execution to comply with Contractor and County IT configuration standards. CSA also provides the foundation for the cloud service catalog presentation, automation, management, and orchestration.

The Contractor team shall manage the server, storage, backup, and networking resource pools along with System Management Software, such as HPE Server Automation software layers. These products shall help to facilitate the day-to-day operational support for the converged infrastructure-based cloud resource pool. They shall automatically deploy predefined Windows and Linux operating systems into the environment via predefined workflows.

Contractor shall deploy monitoring, antivirus, and policy compliance agents as part of the automated workflows. The consistent and reusable private cloud infrastructure shall enable the County to rapidly access the infrastructure when needed. Contractor shall maintain and manage all the software, agents, and monitoring infrastructure of the private cloud.

There are two scenarios of security integration for cloud based solutions:

- In the first scenario, the cloud solution is tightly integrated with Contractor's standard data center security and allows for implementation, testing, and continuous monitoring of controls as required by County policy. For example, the Contractor's Managed Private Cloud allows for this level of integration in which all applicable county policies are implemented.
- In the second scenario, the cloud solution complies with Contractor/County requirements but may not allow for testing and continuous monitoring by Contractor. In this case, the cloud offering is to be vetted so that Third Party assessments take place on a regular basis and that they share the audit reports with Contractor and County. Third Party assessments shall adhere to valid standards such as ISO 27000, ISO 27001, or FedRAMP.

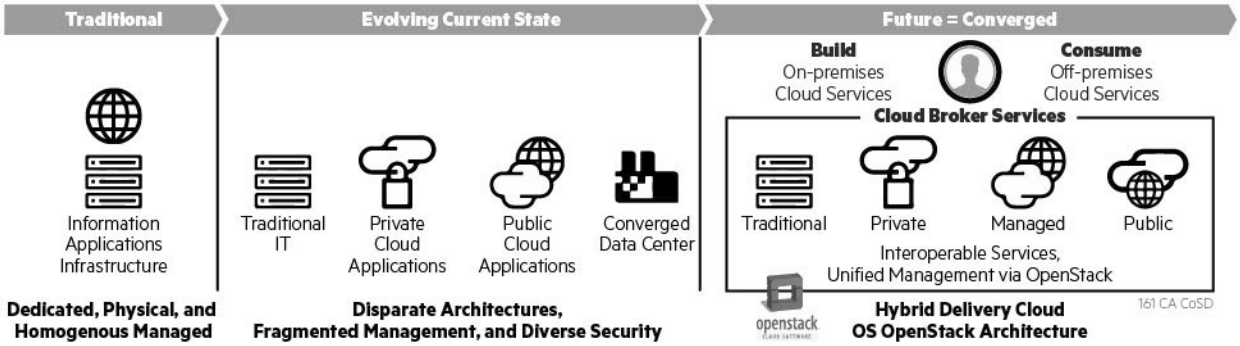
Contractor shall support other key components of the private cloud computing environment, such as CSA and the Private Cloud Portal. Contractor shall support Operations Orchestration, managing the CSA Database, Cloud Controller, and CSA Provider Console, including the following activities:

- Administering the standard Service Request Catalog
- Managing specific CSA settings
- Responding to subscription requests
- Providing lifecycle management of catalog operations
- Supplying standard consumption reports

Implementation of the HPE HMCB shall help Contractor achieve an integrated view of the County's hybrid IT ecosystem and provide the ability to manage VMware-based virtual workloads in the traditional hosted environment both inside and outside of the data center.

With implementation of a hybrid environment in the Tulsa data center, Contractor shall bring application infrastructure improvements throughout the life cycle of an application, whether it is in the MPC or the traditional environment, and whether it resides on a physical server or a virtual host. To improve physical provisioning time, for typical orders of a few servers, Contractor shall keep five (5) spares on hand so that for standard configurations there shall be no wait for procurement. Contractor shall continue to identify opportunities to automate workflows to further improve provisioning of traditional environments to meet or exceed the County's service level requirements. Contractor's complete pre-integrated hybrid cloud solution shall bring to bear data center-wide streamlined service creation, deployment, and monitoring for application workloads, as illustrated in the figure below.

Contractor MPC Standard Building Block and Scale Out Approach to MPC Resources



Contractor shall implement the hybrid delivery architecture shown above under the rightmost arrow ("Future = converged") to bring these disparate silos together. Once in place, Contractor's Cloud Broker shall form the basis to create a continual improvement plan and roadmap. This plan shall unify and bring transparency and consistency of governance to these environments, and Contractor shall help the County target future workloads for the right provider and delivery model.

Contractor's hybrid solution shall provide the following benefits to the County:

- **Faster time to value**. Using the MPC, Contractor shall provide a standard content library with approved County template virtual server (VMs) images that can be provisioned in a matter of hours rather than weeks or months. The standard templates shall allow application solution teams to quickly request web, application and database VMs with preapproved and configured images for the County landscape helping drive the County's "virtual first" strategy.
- **The right hosting solution for any application**. For applications that require a high level of customization, such as use of non-standard platforms, Contractor's traditional hosting service provides this solution.
- **High performance application services:** This shall result in better service to end-users, third parties and constituents of the services.
- **HMCB:** Consolidated management and financial governance of traditional, private, and public cloud hosted environments.

- Deployment plan for resources and use of facilities

Contractor shall provide application infrastructure services for the County applications portfolio in Contractor's Tulsa and Plano data centers, until the consolidation to the Tulsa data center is complete. Contractor shall migrate all workloads from Plano to Tulsa.

Within these environments in Tulsa, the Contractor team, which includes the local team in San Diego, Contractor's service center in Pontiac, Michigan, and Contractor's virtual teams of subject matter experts (SMEs), situated throughout the United States, shall manage and operate the application infrastructure services required by these applications.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall use a life cycle approach to support applications infrastructure. Contractor shall follow an application placement methodology in which Contractor shall assess cloud readiness. Contractor shall look at each County application in the production inventory and analyze where that application would best be deployed based on evaluation of the following types of requirements:

- Regulatory requirements

- Performance requirements
- Adherence to infrastructure standards
- Security and confidentiality
- Availability and reliability

When designing the infrastructure to support an application, Contractor shall determine which tiers are required. The tiers shall include the presentation layer, business logic (application) layer, and the back-end (database/transaction) layer. The infrastructure to support any tier can be either MPC or traditional. The County's network zones shall be supported transparently in both environments.

Prior to migration, Contractor shall build out the MPC and upgrade and expand Tulsa's traditional environment to include the required infrastructure for servers, storage and networking components to accommodate the migration of applications into this facility. As part of the consolidation, Contractor shall analyze the application environment and identify the candidate environments to move into the MPC. When this is complete, candidates from the Tulsa environment shall be moved into the MPC to further consolidate and standardize workloads. Upon refresh and subject to County-defined limitations for periodic refresh cycles, Contractor shall continually evaluate additional application workloads to assess the feasibility of moving these to the MPC. Contractor shall analyze items such as County investment, timeframe for application retirement, if any, and the complexity of the development effort for legacy applications to be re-architected in MPC.

For all application infrastructure upgrades, refreshes, and transformational activities that impact portfolio applications, Contractor shall update and maintain AppsManager with information needed in Runbooks. Application infrastructure examples shall be updated DNS, system patches, and sections for outage and notifications, data center and escalation contacts, application interfaces, AD/service accounts and document links, whether provided in the MPC, traditional hosted, or other cloud environments.

Performance Analysis and Improvement

Contractor shall use a variety of methods to analyze performance.

Reactive Performance Management

Contractor shall implement tools to provide early warning alerts to Contractor that shall automatically contact Contractor to look into a situation where some resource or performance metric has passed a threshold point.

Proactive Performance Management

Contractor shall review the trend analytics and reports on capacity and performance on a daily basis.

Netcool and NNMI shall be used to monitor and assess the data center network devices. Performance issues shall be addressed using standard event management (for non-impacting events, such as threshold warnings) or incident management (for End-User-impacting issues) procedures.

Contractor shall review the results of these analyses with the County and make recommendations for County approval.

Performance improvements, in response to either reactive or proactive scenarios, shall include tuning configuration parameters, adding capacity, or making an architecture change such as re-shaping network traffic or moving data to a different storage tier.

Contractor shall also follow the same methodologies and processes to manage the application infrastructure as Contractor does for infrastructure services.

6.8. Infrastructure Services

6.8.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide infrastructure services such hardware, software, network resources and services required for the existence, operation and management of the County IT and telecommunications enterprise, at both Plano and Tulsa until the data center consolidation is complete. These infrastructure services shall provide the foundation that supports County End-Users, third parties, and constituents. The infrastructure services environment shall be comprised of the hardware, software, storage and support services that underpin the operations of the applications and Dev/Test environments, including:

- Server environments that run the supporting tools, including Service Portal, ITSM systems, monitoring, reporting, analysis and alerting systems.
- Infrastructure that provides software distribution and delivery services for mobile, desktop, and data center server environments.
- Local file and print services, distributed throughout County locations.
- Network infrastructure supporting the data center, such as load balancers, WAN Accelerators and global traffic managers (GTMs).
- Background services for applications, such as backups, batch processing and File Transport Protocol (FTP) services.

The servers for infrastructure services shall reside in both the MPC and traditional hosted environment. Over time, Contractor shall work to optimize and standardize this environment as opportunities arise. Servers that support infrastructure services shall receive the same supporting functions (such as performance and capacity management, and backup and restore) as application servers. Contractor shall make sure that no single points of failure exist that could potentially impact the availability of applications or facilities that support County business.

Contractor shall perform comprehensive infrastructure testing for all components in an integrated environment for compute, storage, network, and database in a physical or virtual environment. Contractor shall maintain documentation that identifies all infrastructure services' hardware versions and software version life cycles so that Contractor may adequately plan timeframes and completion dates to stay within supported versions of both hardware and software. Contractor shall also track hardware and software assets to adhere to the County refresh cycle. ESX servers and network components that comprise the MPC shall be refreshed on the same schedule as their traditional hosting/network counterparts.

Contractor shall deliver skilled operations and engineering expertise to manage and monitor the infrastructure services environment, and apply automation to all processes to the greatest extent possible. Contractor shall deploy monitoring, antivirus, and policy compliance agents as part of the automated workflows. Contractor shall manage the County's server, storage, backup, and networking resource pools and system management software, to facilitate daily operational support.

Contractor shall manage and maintain the County's server (compute), storage, backup, network, and security environments. Contractor shall follow ITIL-aligned processes to determine critical business impact to component or system failures in infrastructure services, and to continuously analyze, identify and remediate single points of failure in infrastructure services.

Computing Services—Contractor shall install, fully manage, and monitor the operating system (OS) instance and the underlying virtual or physical server. Contractor shall also maintain the health of infrastructure assets included in the solution, including server, storage, backup, network, and other devices.

In the MPC and traditional hosted environments, Contractor shall preconfigure the OS image for automated provisioning, provide OS patching and ongoing maintenance including performing all software installations, patching, and ongoing maintenance, and monitor system availability and security. Contractor shall perform root-cause analysis and corrective action of OS, physical and virtual servers, storage, backup and network environment problems, and all other IT Service Management functions.

End-User Software Distribution – Contractor shall design, deploy, and maintain software distribution infrastructure and services for End-User computing services and integrate and perform software delivery for County desktop and mobile devices. Contractor's infrastructure services shall include support for devices on the County Public Library private network.

Operating System Software Support—Contractor shall provide a standard build for, then monitor and manage, virtual and physical operating systems such as Microsoft Windows, Red Hat Enterprise Linux and Oracle Solaris. Contractor shall also support other types of UNIX operating systems and VMware as well as other hypervisors.

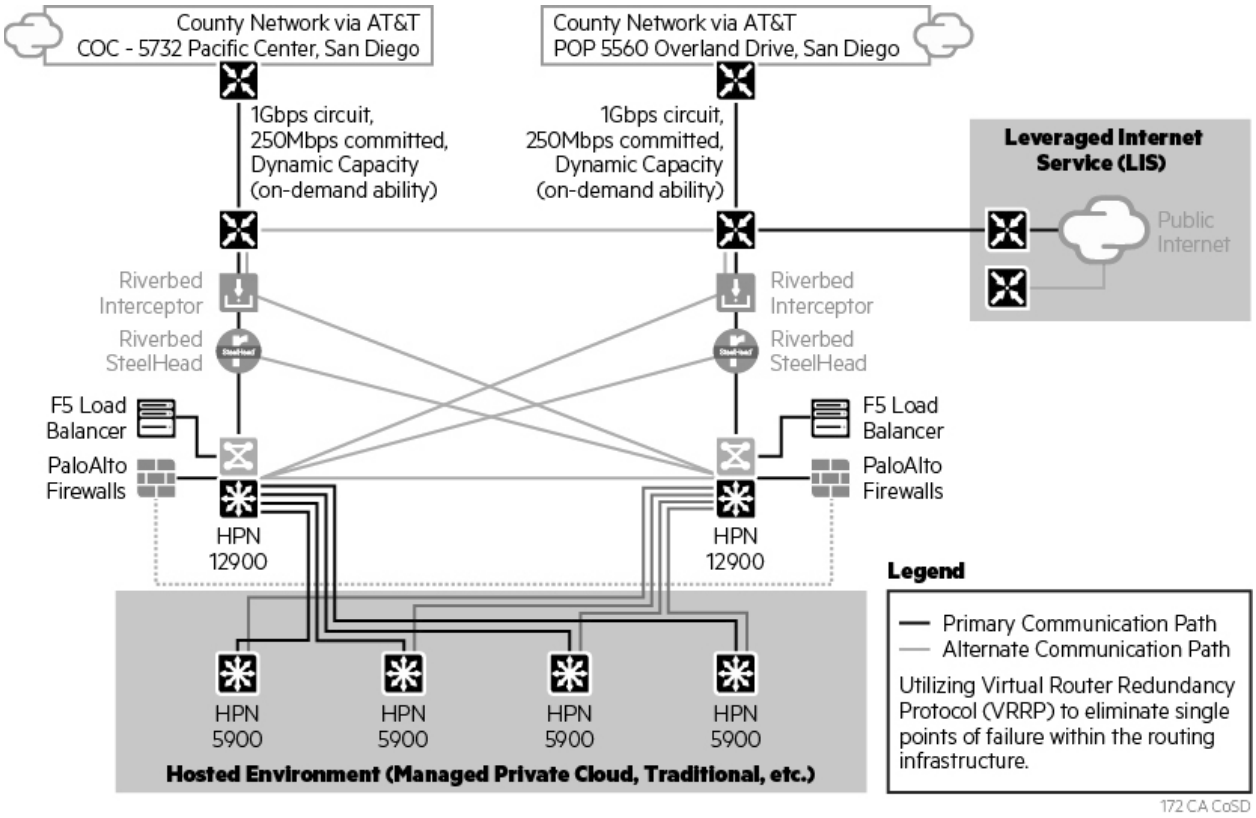
Storage services—Contractor shall use the HPE 3PAR enterprise storage, which is designed for both cloud and traditional environments. The storage shall host operating system images, virtual snapshots, and application data. All operating system images for virtual machines shall boot/reboot from the Storage Area Network (SAN). This architecture enables the server image to be disassociated from the physical hardware, allowing the image move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover for improved availability.

Backup and Restore Services—Backup services for virtual and physical computing services shall provide operating system and filesystem (offline) backup for computing services to enable data restoration after a data loss event. Backups shall be accomplished by copying the specific data to backup media. Contractor shall perform the following:

- Provision backup infrastructure and backup software
- Perform backup management
- Maintain the backup schedule
- Review backup job completion status
- Intervene in the event of backup error
- Store data on disk
- Performs OS, file system, and database restore.

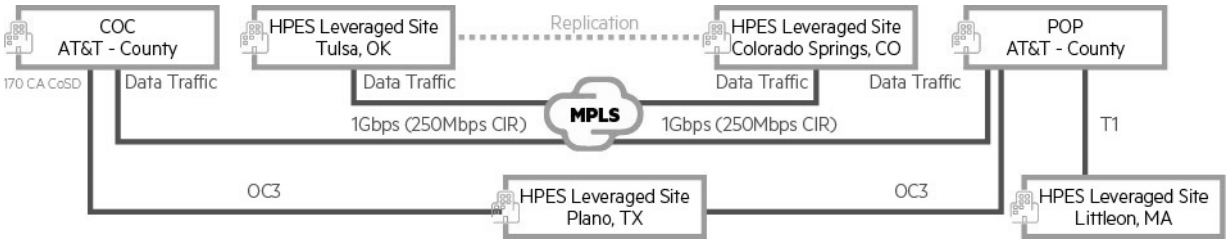
Contractor shall initiate and perform on-demand backups of the County environment. Shortly after the request is submitted, an incremental backup shall begin. For virtual servers, Contractor shall be able to conduct regular snapshot backups of each virtual server instance, with the most recent snapshot being retained for recovery purposes. The snapshot feature shall back up the OS disk and all attached data disks. The figure below illustrates the data center network architecture.

Data Center Network Detail



Contractor shall provide a wide area network service construct with diverse paths and entry points into each data center at Contractor's Tulsa, Oklahoma, and Colorado Springs, Colorado, locations. All circuits shall be in an Active configuration to allow operation. Multiprotocol Label Switching (MPLS) circuits with a 250Mbps committed information rate (CIR) shall be used to connect Contractor's data centers to the County's Pacific Center and Overland Drive locations. Each of these circuits shall allow bursting above the CIR to provide on-demand bandwidth increases. Replication shall occur between the two Contractor data centers via a dedicated 10GB circuit. The figure below illustrates this connectivity.

Data Center Connectivity to the County Network



Contractor's WAN and LAN network infrastructure shall deliver multiple, active network paths with 1+1 redundancy at a minimum, whereby multiple components can fail without impacting end-to-end network availability. This enables Contractor to deliver an environment truly capable of targeting 100% availability.

Scalability shall be delivered through the 1+1 active/active construct. Contractor shall use the HPE 12900 and 5900 series switches to provide a high performance, scalable, and open architecture designed for the County to

leverage for the next decade. The platform shall be purpose-built for the data center around the principles of modularity, extensibility, and agility.

The network shall be designed and implemented with modularity. This enables Contractor to expand in the future in accordance with the forecast workload. It also simplifies network deployment activities. Contractor shall provide an environment with inherent High Availability capabilities, which is concurrently maintainable, and simple and efficient to operate, reducing the risk of administrative error.

In addition to Contractor's LAN and WAN infrastructure, Contractor shall provide a Leveraged Internet Service (LIS).

Connectivity from the County network to the Plano and Littleton data center, required to remain post-transition to support the mainframe and AS400 environment, is depicted in the diagram above; this connectivity shall remain in place for as long as required to support the mainframe and AS400, and shall be decommissioned once the mainframe and AS400 applications are replaced.

Contractor's LIS shall use circuits from redundant ISP providers, terminated on hardened data center infrastructure to maximize reliability.

LIS shall be offered in monthly subscriptions from 1Mbps to 10Gbps for access to applications and servers hosted within Contractor Data Centers. For implementation during Transition, Contractor shall deploy 50 Mbps, consistent with current traffic requirements in Plano and Tulsa; this shall automatically surge if needed, with no additional charges to the County for surge usage.

Network Management Services—Comprehensive network design and infrastructure management services shall enable provisioning of up to 1024 VLANs per server; monitoring and management of data. Contractor shall implement new network technologies across the enterprise, manage disparate networks, and maintain reliable network performance. Contractor's network management services shall provide a centralized and standardized system that automates network management of End-User data, security, and distributed resources. Contractor shall continuously monitor and maintain all load balancers for optimal operational performance. Contractor shall also deploy and maintain application and network acceleration in the delivery of the Services.

Security Services—Antivirus agents shall automatically be deployed and activated in an automated workflow when a server is deployed. Security policy compliance shall check system configurations against security standards at a predefined scan frequency based on Contractor's security best practices. Contractor shall automatically load policy compliance agents as part of the deployment workflow and maintain and manage the security software, antivirus and policy compliance agents, antivirus definitions, and underlying infrastructure to support the security technology. Contractor shall maintain and provide all infrastructure security components including IPS and firewalls.

Data Center Facilities Services—Contractor shall design all the key supply components (for example, power, air conditioning, and wiring) to be redundant. In addition, Contractor shall control access to the data center to prevent unauthorized entry, and provide a robust infrastructure that provides adequate resistance to damage by the elements.

Costs Included in the Resource Unit (RU)

Hardware - This RU shall include the cost of Load Balancers, Network Accelerators, and Facility charges for infrastructure hosted in the AT&T POP.

Hardware costs (servers and storage) for servers designated as Infrastructure; i.e., servers that run the tools used in providing Framework services, or are otherwise used for a purpose other than to run County business applications

shall be included in this RU. Other servers that shall be included in this category are servers that represent a non-variable cost component of another RU; for example, the servers that run the Netmotion and Granicus applications are billed under the Infrastructure Services RU rather than under the RUs specific to those applications because the costs do not vary in linear proportion to volumes. This prevents the possibility of over-billing if volumes grow significantly.

A portion of data center network hardware and circuit cost shall be allocated to all servers. The portion of that cost for the servers designated as infrastructure shall also be included in this RU.

Software - A portion of data center software/tools cost to provide services such as software distribution, performance management, capacity management, and other automation and management functions shall be allocated to all servers. The portion of that cost for the servers designated as infrastructure shall be included in this RU.

Operating system, database and hypervisor software specific to infrastructure servers shall be included in this RU.

Labor - A portion of server, storage and network support labor shall be allocated to all servers. The portion of that cost for the servers designated as infrastructure, as well as the support cost for the network components described in the hardware section above, shall be included in this RU.

- Deployment plan for resources and use of facilities

H Contractor's data center staff in Tulsa, the Contractor local support team in San Diego, and Contractor's virtual team of SMEs, located throughout the continental U.S., shall provide ongoing operations and maintenance of the County's infrastructure.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall operate the Tulsa datacenter in accordance with ISO 27001 and the ITIL framework and best practices. To manage County infrastructure environments, Contractor shall follow ITIL-based service management (event management, and others) best practices.

Contractor shall put in place a process and roadmap to unify and integrate the various providers of services, and develop decision criteria that target workloads with specific characteristics for a specific type of service provider. In addition, continual improvement shall include convergence of tools for a more integrated data center services catalog and more self-service. Contractor shall provide additional self-service capabilities from the Service Portal at the County's pace.

For all infrastructure environments, whether provided in the MPC, traditional hosted, or other cloud environments, Contractor shall provide a robust support service, to include the following processes:

- Hardware installation and configuration
- Hardware and firmware management and support
- OS and layered software product installation and subsequent patching and release management
- Supplier maintenance agreements and coordination of suppliers' activities in support of the applications infrastructure
- Capacity and performance monitoring and management
- Problem monitoring, including proactive hardware support
- Data center facility (floor space, power supply, cooling, wiring) services
- Network integration into the Tulsa data center
- Underpinning services that use the infrastructure services framework (such as directory and domain name management services), described in Section 2.5.

- Refresh of hardware components, at 25% per year for Windows environments and 20% per year for UNIX, Linux, and VMware ESX environments (MPC hardware is included).

These services shall be provided for applications infrastructure, infrastructure services, and development and test services. The work instruction documents for these processes shall be available to the County in the Standards and Procedures Manual.

6.9. Development and Test Services

6.9.1. Process and Procedures

- Description of solution to meet the requirements

Contractor's solution for the County's Dev/Test services shall take advantage of the hybrid infrastructure approach described in the previous two sections, employing both the MPC and traditional hosted environments, with resource pools separate from application infrastructure and infrastructure services. This approach shall provide the unified consistent architecture that makes sure the Dev/Test shall provide an accurate picture of how an application's production environment performs. The MPC environment shall be a highly standardized environment with high redundancy and high availability to eliminate single points of failure. Moving to MPC shall provide streamlined server provisioning, enabling Contractor to provision, scale, and de-provision virtual servers in hours instead of days, once approved by the County. It shall also include tools that simplify capacity and performance management, monitoring, patching, and security and regulatory compliance.

Both the MPC and the traditional hosted infrastructure shall be sized to accommodate the combined workloads from Plano and Tulsa.

The "Dev/Test" RU consists of two logical environments – "Dev/Test" and "Break/Fix." Although there is one Resource Unit for "Dev/Test," the second logical name of "Break/Fix" was added to describe a component of the "Dev/Test" RU for management reporting on utilization and consumption of resources. The logical name "Dev/Test" is used primarily by Applications Development, while the logical name "Break/Fix" is used primarily by the Applications Maintenance and Operations. Details of what is in included in the "Dev/Test" and "Break/Fix" environments are outlined in the appropriate documents.

The MPC environment designed for the County shall provide the following benefits for Dev/Test:

- For Applications maintenance and operations (M&O) Break/Fix environment, dynamic and persistent resources provide a cost-effective solution for certain P1/P2 category applications, Contractor shall keep persistent environments in place, to support rapid test cases, such as performing testing of production fixes in response to incidents. P1/P2 applications shall have persistent Dev/Test environments in the MPC. P1/P2 applications that have been stable for a long time and are not often updated may only need dynamic environments. For these, as well as all P3/P4/P5 environments, Contractor shall take advantage of MPC's elasticity, where Contractor dynamically scales the County's secure, dedicated virtual infrastructure up and down as needed quickly and easily by obtaining and releasing IT computing resources on demand.
- Faster provisioning of hosted application services, and cold storage of dynamic virtual images not in use shall help the County to avoid operational costs and data center footprint associated with paying per-server for idle servers.
- Enhanced scalability and flexibility to adapt to the County's dynamic business demands.
- Security, privacy, and compliance—the MPC infrastructure is 100% dedicated to the County, and Contractor shall protect this behind a highly secure data center firewall. Contractor shall deploy and manage the

technology based on Contractor's extensive security testing practices that meet multi-segment security standards and compliance beginning with FedRAMP Moderate requirements.
- Access to the latest cloud innovations when the County is ready. Contractor shall help the County stay at the forefront of this technology by continuing to offer service and technology enhancements as HPE Labs research and develop next generation cloud systems.
- Integrated with County identity and access management services either through Active Directory or Oracle IDAM.

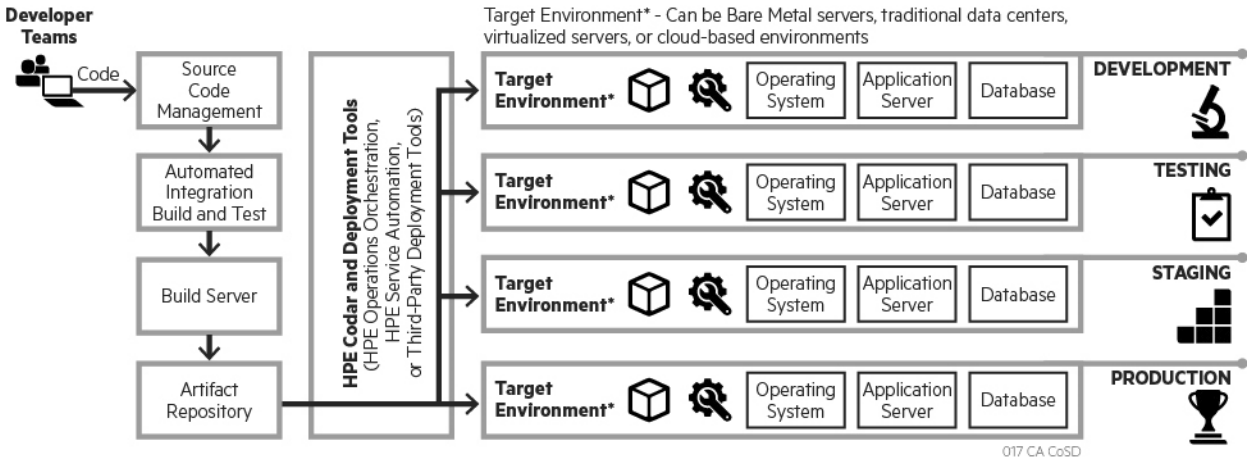
The Dev/Test environment shall be designed to meet County goals for continual improvement and cost effective innovative services to help the County transition to a marketplace of hybrid-provided services governed by Reports 49/50 standards and County IT strategy. Financial governance of the Dev/Test environment shall be through the HMCB and shall provide visibility across the hybrid environment to all Dev/Test resources in MPC and traditional hosted environments as well as public cloud environments.

Contractor's solution shall use the VMware automation built into the HPE Helion Cloud tools.

To further increase the level of automation and improve the Dev/Test environment builds, Contractor shall mature the cloud development, orchestration and delivery tools that shall enable Dev/Test environments to be quickly placed through one-click deployments, automatic rollbacks, and applications promoted across virtual environments. Contractor shall establish modeled environments that shall enable additional consistency through Contractor's automated tools such as HPE Codar and HPE Cloud Automation solution for version-controlled, one-click deployments, rollbacks and promotions.

Employing the same architecture used in application infrastructure services for Dev/Test shall streamline and simplify the migration of applications—from Dev/Test to production. Contractor shall ensure that all individual technical components configured with or added to the services mesh together to achieve the intended results prior to release to the production environment. Contractor shall operate the Dev/Test environment according to all County standards and in close alignment with the production environment. Upon County approval, Contractor shall use the VMware integration capability of the MPC and HMCB to clone production images to the Dev/Test environment.

Automated Tools for Deployment of Environment Models



Contractor's v 4.0 MPC solution is a commercial-release offering and shall be designed as a set of building blocks that can be sized and deployed to fit almost any enterprise's requirements.

Contractor shall provide sufficient SAN capacity in the Dev/Test environment for MPC to store cold virtual machine image files. Contractor shall manage Dev/Test workloads within a SAN-based repository visible to the

private cloud and perform tasks such as boot up and shut down of virtual machine images on-demand. Upon the County's request/approval, the tasks shall commence automatically. The Dev/Test environment shall have interfaces enabling connectivity to the production environment as needed to meet business needs. Contractor shall secure these interfaces with VLANs and access control lists. Identity access management services shall be applied across all County environments, including Dev/Test.

Production and non-production virtual servers in the MPC shall never reside on the same physical servers. If the application moves from the development/test phase to production, by making the test VM itself production, then that virtual server shall be moved into the production farm (cluster) when it goes live.

- Deployment plan for resources and use of facilities

The Dev/Test environment is part of the overall hybrid data center architecture and shall reside in the Tulsa data center.

The Rancho Bernardo lab remains available for integration and testing services and proof-of-concept applications or infrastructure that need to be isolated from the production network.

Resources working in the Dev/Test environment shall include Contractor project managers (PMs), developers, and operations staff, as well as designated County stakeholders during End-User testing phases.

- Processes solution including year-to-year continuous improvement

The methodologies and processes used to manage the Dev/Test Service are the same as those described previously in the Infrastructure Services

As described in the Solution Summary section above, Contractor uses the following methodologies:

- IT Strategy and Architecture (ITSA)
- ITIL framework

As a continual improvement initiative, Contractor and the County shall consider adopting development and operations (DevOps) approach to managing development. Contractor shall incorporate DevOps practices of collaboration, source control, deployments through version-controlled models, and system configurations. DevOps shall work together to design and maintain models and configurations in version control from which automated tools can fetch and deploy.

Specific to the Dev/Test environment, the Contractor team shall create new processes for:

- **Automated Release Management** – Using the approach described in the Solution Summary section above
- **Dynamic Image Management –** Used for turning up and down dynamic images and making sure that cold-stored images are reused (as opposed to creating new images every time) and processes for inventorying and removing cold-stored images. For physical servers, images are not dynamic, but if an environment is targeted for turn-down so that its resources may be reused for another project, Contractor shall have processes and scripts to back it up and remove it from active support status during the time while no projects are using its resources.

When a Dev/Test team needs an environment to support a new release, for example, they shall submit a request for requisite resources through the cloud interface or the traditional request process, depending on the resource needed. Upon approval of the request, and determination that sufficient capacity is available to support it, the resources shall be automatically provisioned in the cloud or the traditional VMware environment (or provisioned with task-level automation in the traditional hosting environment) and the requesting team notified of its availability, measured in hours, not months.

6.10. E-Mail Services

6.10.1. Process and Procedures

- Solution to meet the requirements and the rationale

Contractor shall migrate the existing, traditional-hosted Exchange 2010 email to O365 Exchange Online as a transition project.

Contractor shall manage the current Exchange 2010 high availability environment for email service that includes four Exchange servers each in Plano and Tulsa. Contractor's support shall include mailbox management, OWA traffic, ActiveSync, mail relays, GALsync, and RightFax. Contractor shall provide backup and restore functions, and meet special mailbox recovery and journaling requirements. Contractor shall also meet the current retention requirements of 118 days for deleted items and mailboxes and perform backups every other week and retain tapes for 2 weeks before overwriting.

O365 shall fully meet the County's requirements for email services and shall allow the County to take advantage of additional available functionality in a timeframe convenient for the County.

A full discussion of NetBond is provided in the Network Services Framework.

Rationale:

The transition to Exchange Online shall result in the following changes to the existing environment:

- One hybrid exchange server in Tulsa to maintain the local distribution lists
- The RightFax servers in Tulsa shall be connected to redundant local SMTP relays
- Microsoft shall provide email archiving, journaling and e-discovery services.

Contractor shall provide support for email, even after the transition to O365. The Contractor Service Desk shall own the trouble tickets and resolution from start to finish. Contractor and Microsoft shall use Contractor's ticketing system that is devoted to Contractor client support to meet the County's required SLs.

The following table illustrates how Microsoft Exchange Online meets the requirements of the RFP.

Microsoft Exchange Online and Office 365 Features

Requirement	Solution
With respect to licensing, the County has a Microsoft Enterprise Agreement (EA) in place that includes Office 365. The Microsoft EA also includes licensing for the data center Exchange servers.	Contractor's solution covers the County's existing subscription with Microsoft.
Migrate to the current version of Exchange	All MS office productivity applications such as Outlook are continually updated and patched to the most current version. During the migration to Exchange Online, End -Users shall be updated to the latest version of Office 365 Professional Plus. Office 365 Professional Plus shall be installed on all End-User devices as a part of Transition
Migrate to the current version of Outlook to desktops	
Contractor shall ensure high delivery of cloud based E-Mail Services and complete End-User integration.	
Maintain versions of Exchange within 12 months of new releases	
Maintain patch levels of Exchange within 3 months of any new release	

Appendix 4.3-1 Contractor's Solution

Requirement	Solution
Maintain County retention policies (60 days) without exception	Retention limits can be set across the board or down to an individual mailbox. A County-requested legal hold would be the only exception to the retention policy.
Unlimited Mailbox storage	Contractor shall configure the mailbox to use the archive as the mailbox location to provide unlimited storage.
Unlimited End-User archive storage	
Redundancy built-in to insure minimal down time for E-Mail End-User	MS Office 365 (including Exchange Online) provides 99.95% availability. Their infrastructure is architected with sufficient redundancy and replication to support this level of availability with no data loss due to failures; Contractor provide redundancy of network and surrounding components.
Continuous backup to prevent failure due to data loss	
Contractor shall maintain E-Mail Services so there is not a single point failure thereby assuring County daily use continues to operate during any unplanned event or outage.	
Malware and anti-spam protection at the perimeter and within the Outlook client	Exchange Online Protection (EOP) is included in Contractor's solution and provides malware and anti-spam protection at the perimeter and within the server. Malware protection at the desktop is provided by Symantec Endpoint Protection. EOP also provides the following capabilities: - Journaling - E-Discovery - Archiving - Data Loss Prevention Additional information about Exchange Online security is provided below this table.
Immutably preserve or In-Place Hold for End-User data, as requested	
Protection against unsafe attachments at the perimeter and the Outlook client	
Data Loss Prevention implemented per County policy	
E-discovery implemented and used as requested by the County	
Migration of PST files to Exchange archive	The capability to import PSTs in support of eliminating them from the local environment is available. Contractor shall provide migration of End-Users' PSTs
Elimination of PST files from End-User environment	
Implement Outlook Web Access (OWA)	portal.office.com is the Office 365 replacement for OWA—this is provided as part of the implementation during transition. Portal.office.com will only be accessible using County credentials. The process to enforce policy parameters on OWA is described below.
Lockdown OWA to further protect County information	
Mobile aware and productivity included	Microsoft offers a mobile application suite, including Outlook, or users can access portal.office.com via mobile. The same security capabilities apply.
Contractor shall establish and maintain global directory and synchronize E-Mail directories with all County Departments (e.g. Sheriff, District Attorney, SDCERA) or as specified by the County.	Synchronization is accomplished via Azure AD Connect, which Contractor has already implemented for County users. Additional End-User groups shall be added to the synchronization prior to migrating their mailboxes.
Complete migration of all active E-Mail users	Contractor's transition plan shall migrate all active email users
Contractor shall integrate fax capabilities into E-Mail Services for End-Users	Contractor shall integrate the current RightFax solution with Office 365 using a hybrid Exchange server and SMTP relay in the Tulsa Data Center.

Requirement	Solution
Contractor shall recommend a plan for County approval, and execute the approved plan for integrated digital signing to all mailboxes leveraging County PKI platform.	S/MIME is supported and configurable in Office 365.
Contractor shall recommend a plan for County approval, and execute the approved plan for integrated encryption services on all mailboxes based on leveraging the County PKI platform.	Encryption is provided in Office 365 and can be integrated with CoSign and/or the Symantec solution; Contractor shall provide a plan post-migration for County approval.
Contractor shall ensure through continuous review and report that all End-User mailboxes comply with the County's E-Mail retention policy.	Exchange Online provides administrative reporting and auditing that meets this requirement
Contractor shall recommend a plan for County approval, and execute the approved plan to send encrypted E-Mails to E-Mail addresses outside of the County network.	Cloud File Management provides integration into Outlook, which allows transmission of encrypted content to internal or external recipients which require authentication. Exchange Online Data Loss Prevention (DLP) also provides expiration of protected email and content. Cloud File Management has an "I forgot my password" function to enable self-service reset.
Contractor shall recommend a plan for County approval, and execute the approved plan for the ability of external recipients of encrypted E-Mails with access to encrypted content via an authentication.	
Contractor shall enable End-Users an expiration date for sent encrypted E-Mail messages.	
Contractor shall provide self-help password administration for recipients of encrypted E-Mails that permit passwords to be established and reset.	
Contractor shall maintain a timeline/roadmap of all E-Mail Services Hardware versions and Software version life cycles to adequately plan timeframes and completion dates to stay within supported versions of both Hardware and Software that assists in defining the standards.	For the Office 365 Pro Plus environment, Microsoft typically releases updates on the second Tuesday of each month to the Internet. Microsoft publishes an Office 365 public roadmap that provides visibility into upcoming releases to the cloud environment. Contractor shall maintain a timeline/roadmap of all email integrated hardware and software that support this schedule and release the Office 365 Pro Plus updates to the County End-User environment according to that schedule. A detailed description of the update process is available on Microsoft TechNet: https://technet.microsoft.com/en-us/library/dn761709.aspx and the public roadmap is available here: http://fasttrack.microsoft.com/roadmap Exchange Online updates are released quarterly. More information about Microsoft's update process for Exchange Online is available at https://technet.microsoft.com/en-us/library/jj907309(v=exchg.160).aspx
Contractor shall provide centralized support and tools for E-Mail Services hosted within the data center or hosted outside the data center.	The Service Desk shall provide the single point of contact for all email support, including Office 365 and all surrounding infrastructure, such as network, firewalls, fax equipment, and other supporting components. Through Contractor's enhanced support

Requirement	Solution
Contractor shall maintain and be responsible for all components needed to provide E-Mail Services (e.g. load balancers, firewalls, IPS).	service, Contractor provides agents co-located with Microsoft support teams to make sure that issues that need to be escalated with them are not simply dispatched but are followed through to completion.
Contractor shall provide continuous architecture and management resources to participate in planning of upgrades, refresh and transformational activities related to E-Mail Services.	Contractor's Architecture and Engineering team shall provide these services, in coordination with Contractor's Portfolio teams, Microsoft, and Contractor's other suppliers/partners such as AT&T, Symantec, and RightFax.
Contractor shall continuously investigate emerging technologies and services that improve the overall efficiencies, lowers overall costs and improves business application performance and security	

Office 365 Exchange Online Security

Encryption in Exchange Online. Office 365 encrypts data while at rest on their servers and while in transit between End-Users and Office 365.

Data In Transit. Exchange Online supports certificates using Transport Security Layer (TLS) version 1.0 through 1.2, and has recently moved from Secure Hash Algorithm (SHA)-1 certificate support to SHA-2 (Microsoft began deprecating SHA-1 certificate support in June of this year). TLS 1.2 uses Advanced Encryption Standard (AES) with 256-bit length cipher key. Microsoft begins with the strongest cipher key and algorithm and negotiates the proper level with the receiver. There are three types of encryption options with Exchange Online, as follows:

- Office Message Encryption (OME)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Information Rights Management (IRM)

Data-At-Rest. Email data at rest is encrypted using BitLocker Drive Encryption at Microsoft Government Community Cloud Data Centers on hardware using Trusted Platform Module (TPM) version 1.2.

Anti-Malware and Anti-Spam. Users on Exchange Online with Exchange Online protection have their email messages automatically protected against spam and malware. The service has built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect the County from spam. Exchange Administrators do not need to set up or maintain the filtering technologies, which are enabled by default; however, Contractor shall make company-specific filtering customizations in the Exchange Admin Center (EAC) or via remote Windows PowerShell, as required.

Spam shall be prevented as follows:

- **Connection filtering:** Checks the reputation of the sender before allowing a message to get through. Contractor is able to create an allow list, or safe sender list, to make sure that users receive every message sent to users from a specific IP address or IP address range. Contractor can also create a list of IP addresses from which to block messages. Since the license includes Advanced Threat Protection (ATP), connection filtering is used by *spoof intelligence* to create allow and block lists of senders who might be trying to spoof the County's domain.
- **Spam filtering:** Checks for message characteristics consistent with spam. Contractor can change what actions to take on messages identified as spam, and choose whether to filter messages written in specific languages,

or sent from specific countries or regions. Contractor can also turn on advanced spam filtering options if the County wants to pursue a more aggressive approach to spam filtering. Additionally, Contractor can configure End-User spam notifications to inform users when messages intended for them were sent to quarantine instead. From these notifications, End-Users can release false positives and allow Contractor to report them to Microsoft for analysis.

Office 365 Exchange Online can also monitor outgoing messages to determine whether they are assuming the characteristics of spam, and allow Contractor to act quickly. Contractor can further enhance spam filtering by creating custom Transport rules based on County policies. For example, Contractor can use Transport rules to set the spam confidence level (SCL) value for messages that match specific conditions.

Malware shall be prevented in the following ways:

- **Layered Defenses Against Malware:** Multiple anti-malware scan engines help protect against both known and unknown threats. These engines include powerful heuristic detection to provide protection even during the early stages of a malware outbreak. This multi-engine approach has been shown to provide significantly more protection than using just one anti-malware engine.
- **Real-time Threat Response:** During some outbreaks, the Microsoft anti-malware team may have enough information about a virus or other form of malware to write sophisticated policy rules that detect the threat even before a definition is available from any of the engines used by the service. These rules are published to the global network every 2 hours to provide the County with an extra layer of protection against attacks.
- **Fast Anti-Malware Definition Deployment:** The Microsoft anti-malware team maintains close relationships with partners who develop anti-malware engines. As a result, the service can receive and integrate malware definitions and patches before they are publicly released. Contractor's connection with these partners often enables Contractor to develop Contractor's own remedies as well. The service checks for updated definitions for all anti-malware engines every hour.

As part of the County's Advanced Threat Protection (ATP) subscription, there are further protections available. ATP helps prevent zero-day malware attacks in the County's email environment. Contractor is able to set up separate policies for ATP to check either links or attachments or both. Each policy can be applied to a specific set of End-Users, at County direction.

ATP aids in both email delivery and Web browsing from links in emails as follows:

- **Email Delivery**: If the safe attachments policy that applies to a particular recipient has an action of "Block," the email shall not be delivered until the attachments can be detonated by the safe attachments technology in EOP. Safe attachments shall launch a unique hypervisor to open the attachment. This can result in a delivery delay of 5 to 30 minutes for each mail evaluated by safe attachments.
- **Web Browsing (Safe Links)**: If a link points to a website recognized as not malicious, *Safe Links* adds very little latency to loading the target page. If the link points to a website recognized as malicious, the End-User is routed to a warning page and has to go through it (if click-through is enabled) to continue on to the site.

Exchange Online is a highly secure email platform with built-in encryption, anti-malware, and anti-spam. Any system is of course only as secure as its weakest link, and typically that link is at the client level. Microsoft has continually enhanced and hardened its mail clients, and Outlook on Windows as well as the Outlook app on mobile platforms is a highly secure portal to the County's email.

Outlook Web Access (OWA) has been Microsoft's web-based email solution for years; because it has been optimized for multiple browsers and versions of HTML, it is perceived as being less secure than other ways to get email. Contractor does not disagree with this perception. If one needs to use OWA, however, there are few methods to make its use more secure. The most secure way to access web-enabled clients is of course multi-factor authentication (MFA), but Contractor acknowledges that MFA is not a preferred approach at the County, so

Contractor is not recommending it. Contractor's recommendation therefore stands that, to maintain a highly secure email environment across the entire chain, it is most prudent to use Microsoft's dedicated client apps.

For End-Users who require OWA access, various limitations can be configured using the owamailboxpolicy parameters. For example, OWA on Office 365 Exchange Online can be configured to not allow downloading of any attachment while using OWA. It is configurable in two ways:

- via the GUI (basic on/off)
- via Powershell commands for owamailboxpolicy (which provides more options).

DirectFileAccessOnPublicComputersEnabled	Specifies left-click and other options available for attachments when the End-User has signed in to Outlook Web App from a computer outside of a private or corporate network. If this parameter is set to $true,Open and other options are available. If it's set to $false, the Open option is disabled.
DirectFileAccessOnPrivateComputersEnabled	
ForceWacViewingFirstOnPublicComputers	Specifies whether an End-User who signed in to Outlook Web App from a computer outside of a private or corporate network can open an Office file directly without first viewing it as a webpage.
ForceWacViewingFirstOnPrivateComputers	
ForceWebReadyDocumentViewingFirstOn PublicComputers	
ForceWebReadyDocumentViewingFirstOn PrivateComputers	Specifies whether an End-User who has signed in to Outlook Web App can open a document directly without first viewing it as a webpage.
WacViewingOnPublicComputersEnabled	Specifies whether an End-User who has signed into Outlook Web App from a computer outside of the corporate network can view supported Office files using Outlook Web App.
WacViewingOnPrivateComputersEnabled	

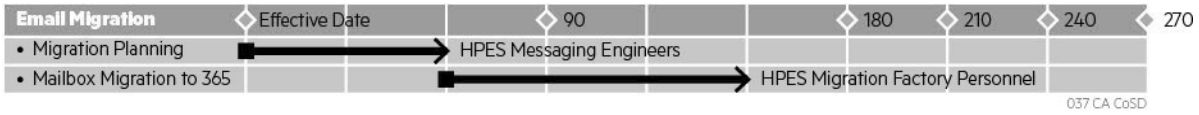
WebReadyDocumentViewingOnPublicComputersEnabled	
WebReadyDocumentViewingOnPrivateComputersEnabled	Specifies whether WebReady Document Viewing is enabled when the End-User has signed in from a computer outside of the corporate network.

- Deployment plan for resources and use of facilities

Contractor's approach to O365 deployment is a repeatable process that Contractor developed through numerous successful migrations, including the Contractor corporate email transition. Referred to as the Migration Factory, it is a standardized service that uses specialized tools running on temporary servers to move email boxes from traditional Exchange servers to the Microsoft cloud. Contractor shall complete the migration virtually, and at the Tulsa data center.

The migration planning process, shown in **Error! Reference source not found.**the figure below which Contractor anticipates to last 60 days, begins at the Contract Effective Date with Contractor's messaging engineers assessing the environment, determining the migration infrastructure need, setting up the temporary infrastructure, and developing a mitigation strategy to address any identified issues. With the migration infrastructure in place, the Migration Factory takes over, moving over email boxes quickly and seamlessly. Contractor expects the migration to occur during an 8 to12 week period.

Email Migration Timeline



Contractor shall provide project management support. Contractor's PM shall guide the process, and County personnel shall be supported through the normal Service Desk for any issues that might arise from an End-User access standpoint.

Contractor shall provide Enhanced Support for Microsoft Office 365. This service is a bridge between Contractor's Standard Service Desk services and the services provided by Microsoft. This is a team that is located in Redmond, WA, with Microsoft. The table below provides a list of the services provided by that team, showing the delineation between Contractor-provided support and support provided by Microsoft. The costs of these services are allocated between the Email RU and the User Data RU (Refer to Transformation Services for a description of this Service).

Contractor and Microsoft Support Responsibilities

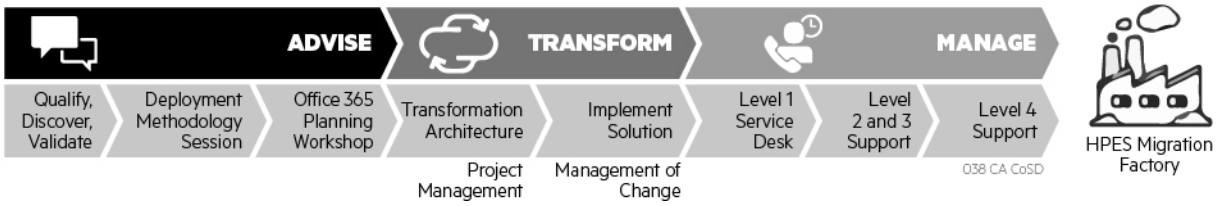
Roles or tasks	Contractor	Microsoft
Contractor and Microsoft Office 365 support team	– Contractor presence in Microsoft Redmond office – Shared document repository – – Knowledge databases, process documents, issue tracking – Weekly team meetings to review tickets, ongoing issues, planned changes, process improvements	
Office 365 service monitoring **Microsoft initiated triage and incident ticket management**	– Action tickets for hardware investigation and repair – Communicate any Office 365 service issues to the County	– Monitor services and platform, hardware, and network – Escalate ticket via case exchange to Contractor
County or Contractor initiated triage and incident ticket management	- Troubleshoot and provide resolution - Escalate via Contractor and Microsoft case exchange - Communicate resolution to the County	– Responsible to troubleshoot and work with Contractor to resolve the incident – Communicate the resolution to Contractor
Post incident time line and summary	Communicate post incident and prior to release of Microsoft Post Incident Response (PIR)	Review time line and summary with Contractor
Post incident response (PIR) and root-cause analysis	– Communicate to the County – Request Microsoft PIR on behalf of the County	– Responsible to develop PIR – Communicate with Contractor

Reporting	– Active and inactive mailboxes – Types of mailbox connections – Mailbox usage and mail activity reports – Mailbox administration activity reports – Mail Security reports – Mailboxes marked for eDiscovery and Litigation Hold – OneDrive for Business sites deployed – OneDrive for Business storage	– Service level availability compliance – Incident reporting – Volume and resource utilization – Post Incident Response and root-cause analysis

- Solution including year-to-year continuous improvement

The O365 Transformation methodology follows Contractor's standard process to advise, transform and manage, illustrated in the figure below. Messaging engineers shall conduct due diligence on the current environment, and prepare the infrastructure and tools that the Migration Factory personnel shall use to move from Exchange 2010 to Exchange Online. As groups are migrated, Contractor shall move into the manage phase, providing support for the entire Office 365 suite from Contractor's Service Desk to Contractor's Contractor/Microsoft co-located support group in Redmond.

Contractor Transformation Methodology



6.11. Unified Communications Infrastructure Services

6.11.1. Process and Procedures

- Description of solution to meet the requirements

With the transition to O365, the vast majority of the County's email shall come from Microsoft's Government Community Cloud, as well as the Lync/Skype for Business infrastructure.

While most End-User experience with UC is local, the underlying functionality shall be delivered from the Microsoft Government Community Cloud. Contractor shall continue to support Avaya phones at the desk and from the AT&T POP in San Diego.

Hosting UC in the cloud is the most-cost effective and technically feasible approach as this architecture is designed for Cloud Delivery.

- Deployment plan for resources and use of facilities

Aside from a single hybrid Exchange server and an email relay in the Tulsa data center, almost all of the data center Services infrastructure for Unified Communications shall be in Microsoft's Government Community Cloud.

Some features of the Government Community Cloud shall be as follows:

- The County's content is stored within the U.S.
- Access to County content is restricted to screened Microsoft personnel.
- Office 365 Government complies with certifications and accreditations that are required for U.S. Public Sector (USPS) customers, such as FedRAMP Moderate.

Lync/SfB functionality shall be, by the end of transition, on O365 Exchange Online also.

6.12. Storage Services

6.12.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide storage capacity to support Tier 1, Tier 2, and all dependent applications in the Tulsa data center using a dedicated SAN. The 3PAR P20000 shall have a 5.6TB of Solid State Disk (SSD) storage for 3PAR metadata. Service storage tiers shall be provided as follows:

- Tier 1 storage in the Tulsa data center shall be configured using low cost 10,000 RPM drives, blended with 9.6 TB of flash storage, that are thickly provisioned and shall provide higher performance at a lower cost than the current 3PAR with 15,000 RPM drives.
- Storage for Tier 2 applications, shall use 10,000 RPM disk drives when thinly provisioned or combined with 7200 RPM disk drives.
- Contractor shall also use 7200 RPM disk drives for archive storage that includes low performance, End-User replicated or infrastructure services.

Contractor shall use the SAN 3PAR array to develop, install, and maintain Wintel and UNIX application infrastructure storage. In some cases, direct attached storage may be required for ongoing service support. Contractor shall work with the County to develop plans to migrate all services requiring storage to the SAN storage solution.

Contractor shall refresh the EMC Centera for the immutable storage tier in the Tulsa data center and at the DR site. The immutable storage shall be replicated from the Tulsa data center to the DR site to ensure a copy of the documents on immutable storage are available during a DR event.

At the document processing center (DPC) Tier, Contractor shall use a storage cache for scanned paper documents that shall be transferred to immutable storage in Tulsa.

Rationale: Tiering Level.

The storage solution provided is a 3PAR 20000 with the same storage tiers provided from 10,000 RPM drives and 7,200 RPM instead of the 15,000 RPM and 7,200 RPM drives. This is possible because the new 3PAR 20000 uses an internal infrastructure to achieve better performance using 10,000 RPM drives. The architecture features the HPE 3PAR Gen5 Thin Express ASIC for hardware accelerated thin technologies, including inline deduplication and 5.6TB of flash storage. Using 10,000 RPM drives provides a lower price per GB of storage at a higher level of performance.

The 3PAR 20000 solution with SSD disk drives, 10,000 RPM disk drives, and 7200 RPM disk drives was selected to provide better performance with lower cost disk drives than the current 3PAR P10000 with 15,000 RPM and 7200 RPM drives.

The current 3PAR P10000 storage is using a maximum throughput of only 2450 KBs per second, and the 3PAR 20000 with 10,000 RPM drives is able to provide throughput of 2438 MBs per second—a rate that is nearly 1,000 times greater than the Country is using in their current storage solution. Providing more than 1,000 times the performance than the Country is using would not be money well spent, and providing 10,000 RPM drives shall more than meet the performance that the County requires.

The figures below were generated from the County's recent storage activity. Performance data from the two current 3PARs were used to simulate the expected performance of the new frame. The current Tulsa and Plano 3PAR P10000 reached a peak of ~2450 KBs per second, while the 3PAR 20000 10000 RPM drive storage is capable of 2438 MBs per second. The 3PAR 20000 is the latest innovation in enterprise storage from HPE. It is the evolution of the time-tested 3PAR storage, so there is little risk to the County by refreshing this storage. Primary data (all 3PAR-based tiers) is replicated to the DR site for applications requiring a 48-hour RTO. **Error! Reference source not found.** summarizes performance of 3PAR 20000 with 10000 RMP drives.

Performance Summary 3PAR 20000 with 10000 RMP Drives

Drives	Quantity	Model	RAID	Workload	I/O size	R/W	MB/S	IOPs
SAS	608	1.2TB SAS 10K SFF	RAID5 (7+1)	Random	32K	60% Read	2,438	30
SSD	32	400GB SSD SFF	RAID5 (3+1)	Random	32K	50% Read	4,712	150,796

EMC Centera was chosen for immutable storage. EMC professional services shall be used to install, configure, and migrate the existing immutable storage environment to the refreshed environment.

Contractor selected this storage solution because it delivers a cost effective approach through the use of different types of storage media aligned to meet the criticality of the applications being stored. In combination with the MPC storage capabilities, the storage capacity shall provide the flexibility desired by the County because it can be allocated as needed to meet changing requirements.

- Deployment plan for resources and use of facilities

With consolidation of the data centers to Tulsa, storage shall be provided at Tulsa and at the DR site in Colorado Springs. Contractor shall provide storage administrators in Tulsa and a supplemental staff in San Diego to support all County locations. All of these sites shall be access controlled to restrict physical access only to people who need it.

Contractor's San Diego storage team shall have overall storage management responsibilities as the central storage management point for the County.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor shall follow established and proven methodologies and key process in all aspects of operations and maintenance (O&M) support, and Contractor shall fully support the County as described below.

- Contractor shall utilize an ITIL framework, Contractor's proven SOPs, industry standard best practices and County policies, processes and procedures to provide storage and innovative, proactive, and responsive O&M.

- Work with the County to develop plans to migrate service from direct attached storage to SAN storage.
- Refresh, support, and manage DPC storage.
- Work with the County to make sure application infrastructure services Contractor SAN storage.
- Support the traditional data center and MPC in Tulsa using the same SAN 3PAR to provide a centralized storage services solution managed by a single SAN administration team.
- Provide usable capacity reports to the County not to include replicated, backup, or DR data storage.
- Provide 20% year-over-year storage growth for 5 years to accommodate the County's business growth.
- Produce storage services reports by storage tier to the Business Group, department, and End-User levels.
- Provide OneDrive for Business for End-User unstructured data storage on Microsoft's Government Community Cloud. User can log into the OneDrive for Business portal to monitor and self-manage OneDrive storage. Contractor shall work with the County to provide self-service reporting and self-service management in other areas of storage services. Initially this shall be access to regular monthly storage reports via the Service Portal, but if desired, Contractor can expand this to include ad-hoc reporting.
- Work with the County to lower the cost of storage.
- Continually evaluate, evolve, and deliver plans to reduce data loss for storage services.
- Produce and submit recommendations on storage services architecture.
- Produce and submit plans on shared storage services consolidation and application server migration to shared storage services environment annually.
- Produce and submit storage services policies and procedures.
- Produce and submit storage services reporting policies and procedures.
- Produce and submit storage services refresh plan annually.
- Produce and submit plans for meeting storage demands.
- Produce recommendations for process improvement in backup and recovery for storage services assets.
- Recommend and submit recovery policies/procedures for storage services assets.
- Produce and submit recommendation on capacity management.
- Produce and submit plans to add storage.
- Plan and schedule all storage-related software/driver/microcode patching and upgrades.
- Design and implement recovery processes based on approved policies/procedures.
- Design and implement storage services management processes based on approved policies and procedures.
- Implement storage services reporting.
- Design and implement storage consolidation based on approved recommendations.
- Deploy, manage, communicate, and report on activities related to storage service refresh
- Design and implement storage services provisioning and allocation processes based on approved policies
- Design and implement capacity management
- Implement approved Storage services policies and procedures
- Implement necessary physical and logical security to protect the County's data (through access controls, storage network, and host-based allocation controls, SAN zoning and host/array-level logical unit [LUN] masking).
- Provide support, including break-fix, for all storage services assets.
- Manage and affect the appropriate resolution of Incident events until the operation of the storage is returned to normal by following customized procedures as well as resolving Incidents upon an automated or manual detection of an event related to storage components
- Manage and support the storage services,
- Produce and submit monthly storage services reports,
- Support storage services refresh,
- Perform and support media management activities for storage services
- Manage and support the media requests
- Provide data storage services (such as RAID groups, storage pools, LUNs, presenting— masking and zoning, reclamation, optimization—tiers, deduplication, thin provisioning, among others)
- Perform tapes mounts as required.
- Perform special tape shipments as requested.

- Provide options for on-premise and offsite data backup storage.
- Provide backup and restore options such as single End-User restores.
- Load and manage third-party media as required.
- Prepare and manage media for use by microfiche service.
- Manage and perform file transfers and other data movement activities related to break/fix or consolidation of storage services assets.
- Perform data backups of storage services per approved policies and procedures.
- Perform recovery processes on storage services assets.
- Perform storage utilization management.
- Manage and maintain all storage services assets and services.
- Produce and submit storage services management reports,

Classification of County data to match required storage tiers.

Classification can imply the County's standard sensitivity classification structure: Public, Sensitive, and Confidential; however, classification can also be extended to permit very granular categorization to support specific policies.

Contractor shall tag documents as they are ingested using a technology-oriented approach to analyze and auto-classify the data.

Contractor's structured four-step process for data classification shall include the following:

- **Understanding the Landscape** – The process begins by gaining insight and understanding of the legacy and "dark data" landscapes. Contractor defines dark data as information assets collected as normal business activity, but these are generally not used for other purposes. Contractor then creates a Solution Roadmap illustrating the go-forward plan and Return on Investment (ROI) for the organization. For the County, Contractor shall accomplish this by sampling approximately 1 TB of data currently residing on the County's existing file share environments. The assessment shall showcase where unstructured data exists and how frequently is it being referenced/used so that intelligent decisions can be made around data management, archiving, retention, and retirement.
- **Develop data categories** – Using automated tools and common categories, Contractor develops a set of categories specific to the County such as Public, Sensitive, and Confidential. Contractor selects a set of representative documents from the County's data repositories to use for training and benchmarking. This makes certain that the categories created are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content. Preparation of these draft categories shall not affect documents in production systems.
- **Refine and Test** – To determine the relevance of the categories to enterprise documents, refining a category is done by adjusting the weighting of a term, the selection threshold, or by adding a field text. These activities can be done individually or in combination. A category can be published, making it available for use in automated policy execution against content managed by the tool suite.
- **Auto-Classification (requires optional Transformation project)** – Once unstructured data is categorized; Contractor applies policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents. Using the desired tool suite, Contractor can automate policy application and govern all aspects of the information lifecycle including deletion prevention, storage management, and ultimately disposition management by applying policies at data creation. Additionally, de-duplicating unstructured data across repositories helps to minimize storage costs and reduce discovery times.

Use of Tools

Contractor shall use tools native to 3PAR that are included in the software of the storage devices.

The 3PAR provided in this solution shall be capable of creating thinly provisioned volumes. The Contractor storage team shall be well-versed in managing these volumes, including close monitoring of volume growth that results in having storage available when needed. Traditional provisioning of storage volumes generally results in large amounts of unused storage that has already been dedicated to a host. Thin provisioning allows for over allocation of the 3PAR storage array and reduces the County's cost by delaying physical storage increases.

The 3PAR shall also have auto tiering capabilities with flexible configuration rules that allow for internal automatic migration, lightly accessed data on high performance, high cost storage to more cost effective, lower performing storage when the need for high performance storage is not warranted, based on the auto tiering configuration. The auto tiering configuration is flexible and allows Contractor to adjust the data migration criteria to rebalance data and free up higher performance storage as needed.

HPE 3PAR System Reporter Software shall be used to automatically collect data on a number of different object data points in the background. The Storage Administrator shall use the 3PAR StoreServ Management Console (SSMC) or the 3PAR Command Line Interface (CLI) to display and report on collected data from an array. Using the SSMC, graphical reports are available for the following metrics.

• Historical data (Performance, Histogram, Capacity)

• Real time data (Performance)

HPE 3PAR System Reporter is a feature-rich analytical engine, which helps Contractor interpret and respond to collected performance data and make sure the Portfolio Applications are performing optimally in the environment.

6.13. Backup and Recovery Services

6.13.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall continue to create backup schedules and policies for the County's data. Contractor shall monitor the backup infrastructure, follow the change management process, facilitate backup completion, and restore backup data on a consistent basis by performing backup restore tests at least once per quarter. The BUR solution shall be adaptable to a non-disruptive transition of services.

Contractor shall provide the current BUR services at the Plano and Tulsa data centers and at the County's sites.

In preparation for the data center consolidation, Contractor shall provide planning support to the County and minimize disruption as workloads and technologies evolve while providing O&M support during transition without interruption.

The existing production backup sets shall be copied to the new solution so that no backup set data is lost during transition. A StoreOnce VTL at the DR site shall join the backup environment as a replication target. Backups shall be replicated to the DR site. Full replication of backups shall serve two purposes:

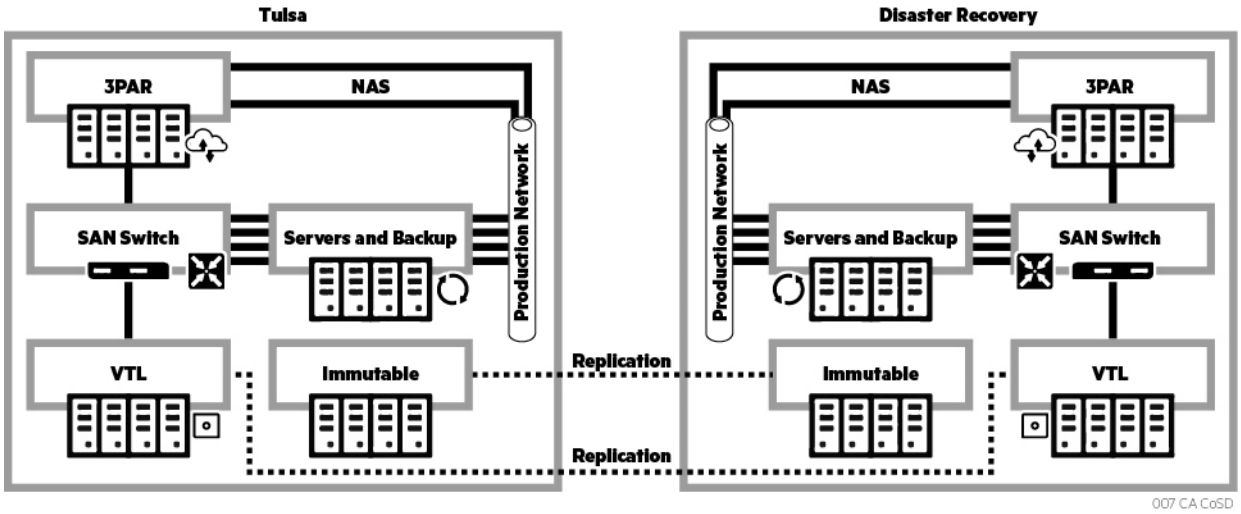
- For applications that require a 72-hour or greater RTO for DR, these backups shall be used to restore service at the DR site.

For all applications, the duplicate backup system provides restore capabilities in the event the primary system is unavailable for an extended period of time. As services are migrated from Plano to Tulsa, Contractor's backup administration team shall create the service's schedule and policy in Tulsa and remove the service backup schedule and policy in Plano for those servers that have completed migration. These backup sets shall be

replicated to the DR site as they are created. When all Plano services are successsfully migrated to Tulsa, the backup environment in Plano shall be decommissioned.

. Contractor's solution shall incorporate 100% duplication of BUR data for the production data center at the DR site. The information shall be replicated between the sites using a dedicated network connection. The backup sets shall be stored in a Virtual Tape Library (VTL) at both locations. **Error! Reference source not found.**The figure below illustrates this solution.

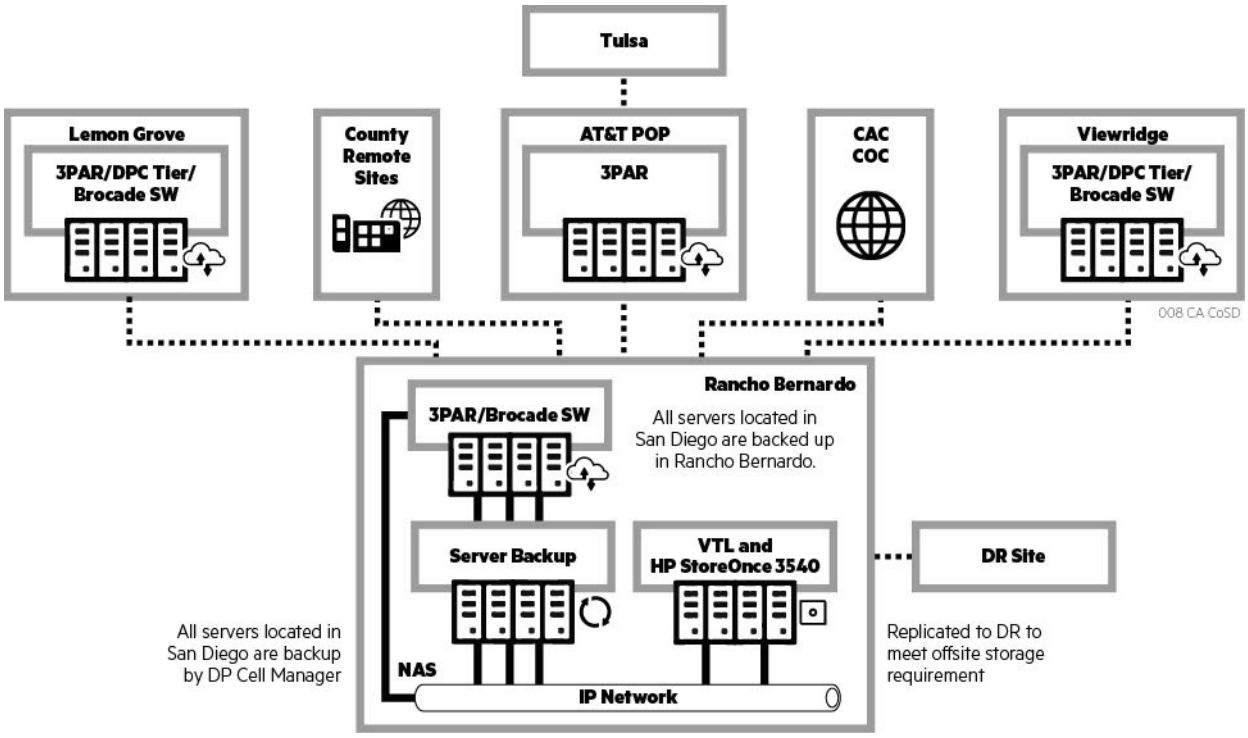
Future Logical View of Data Center Mid-range Server Storage / BUR



Contractor's BUR solution shall provide 100% redundancy of backups in the Tulsa data center and the DR site, providing secure off-site storage of backup data, improved reliability, and quicker data recovery.

In the County's document processing centers, Contractor shall create and consolidate backups at the Rancho Bernardo site using a small disk-based VTL, which shall be refreshed with a replacement of similar size. These backup sets shall also be replicated at the DR site in Colorado Springs. The figure below provides an overview of this solution.

Future Logical View of Document Processing Centers Storage / BUR



Contractor's BUR solution for the data processing centers provides added reliability by backing up servers to Rancho Bernardo and replicating those backups for off-site storage at Colorado Springs.

Contractor shall perform backups of the AT&T POP, Lemon Grove, Viewridge and Rancho Bernardo (collectively known as the San Diego sites) in Rancho Bernardo. Contractor shall copy the existing Rancho Bernardo backup data sets to the replacement VTL to prevent backup dataset loss during the refresh. During the transition period, Contractor shall also replicate the Rancho Bernardo backups to the DR site for off-site retention. This approach provides several advantages:

- Elminates the need for a physical tape library and physical backup tapes, reducing the time required and complexity associated with performing backups.
- Eliminates the need to transport tapes for off-site storage by taking advantage of the DR site to perform this storage function.
- Speeds data restore activities by eliminating the time required to obtain backup tapes from a remote storage facility.

When the data center consolidation is complete, the production and Dev/Test, storage and BUR infrastructure, and O&M support shall be provided in Tulsa, with DR capabilities in Colorado Springs, Colorado. The Contractor backup administratiom team shall continue to provide centralized backup and recovery management from any location because all backup shall be to VTLs and replicated to the DR site over a dedicated replication network connection, eliminating any local tape handling requirements. All County data shall be backed up, as required.

Built on HPE Data Protector 9.0 software, Contractor's BUR solution shall provide comprehensive functionality designed for enterprise environments using a dynamic and agile data protection strategy. HPE Data Protector servers shall integrate with LDAP authentication services and support file inclusion and exclusion as an extra level of control. The Contractor administration team shall provide for auto-discovery of virtual servers, supports single-pass image backups of virtual servers, shall provide integration with HPE Data Protector with Oracle RMAN, and shall integrate with VSS to backup Shadow copies that have been created. It shall provide

standardized backup and recovery across applications, formats, storage platforms that include disk, snapshots, tape, and cloud, with improved reliability if it becomes necessary to load stored backup data in the event of a failure. It shall provide standardized backup and recovery across applications, formats, storage platforms that include disk, snapshots, tape and cloud, with improved reliability if it becomes necessary to load stored backup data in the event of a failure. HPE Data Protector shall provide real-time operational intelligence through a customizable BUR dashboard, that Contractor shall publish on the Service Portal.

Backups shall be weekly full backups and daily incremental backups. The backup retention period shall be customized within the policy that defines the backup, based on the type of data being backed up. Custom retention periods can be defined for specific Portfolio Applications, with County approval if the retention period requested is outside of the policy. Contractor shall categorize the types of data requiring backup and retention timeframes, as detailed inthe table below when developing the BUR solution.

Types of Data Requiring Backup and Retention Timeframes

TYPE OF DATA	RETENTION PERIOD
User unstructured Data (NAS): • H: Drives • S: Drives • Application Dev/Test • Application Production	90 days
Exchange 2010 (Email) • All Passive databases	14 days
Structured Data (Databases) • Dev/Test • Production	30 days
Application Servers • Dev/Test • Production	30 days
Infrastructure Servers • Domain controllers, SCCM Servers, Citrix, among others	30 days
Immutable Storage • Host based backups	30 days

For the County, the hardware solution shall be comprised of:

- HPE Data Protector Servers (7 cell managers and 9 media managers)
  - Cell managers are the servers that control, monitor, and store all backup object information
  - Media manager servers connect to backup target medion (disks, virtual tape or physical tape media) to access those media destinations.
- HPE StoreOnce B6600 disk-based backup media target, or VTL, in Tulsa. All Tulsa data center backups shall be replicated to a VTL in the DR site in Colorado Springs
- Contractor's StoreOnce 3540, at the Rancho Bernardo site, shall also be replicated to the DR site for off-site backup set protection.

Additional functionality provided by this solution includes the following:

- SharePoint – granular restore
- VM Server – snapshot restore

- Synchronized backup application for the Enterprise Document Processing Platform (EDPP).

  For cloud applications hosted outside of the Contractor data center, backup options shall be provided by the Cloud Service Provider.

Rationale: This approach shall provide improved reliability by eliminating a point of failure present if portions of data are backed up by different sites.

- Deployment plan for resources and use of facilities

Until the data center consolidation is complete, BUR services shall continue to be provided in the Plano and Tulsa data centers and the County document processing centers at Lemon Grove and Viewridge.

After the data center consolidation, Tulsa shall serve as the production data center and Colorado Springs shall be the DR site. The County document processing centers at Lemon Grove and Viewridge shall continue to serve the same functions. At this time, the space provided for the County in the Plano data center shall be released, and connectivity from the AT&T POP shall serve Tulsa only.

Contractor shall provide backup administrators in Tulsa with additional local staff to support the San Diego sites and shall be responsible for management of the immutable storage in Colorado Springs. They shall also manage the replicated images, 100% of which shall be replicated to the DR site.

SAN and SAN storage hardware shall be managed by Contractor USPS resources.

- Key methodologies and processes in solution including year-to-year continuous improvement

Contractor's BUR processes shall address the following types of backups:

- Virtual Servers – Snap Shot is VMware based for data within the VMware image, includes system state.
- Physical Servers – Host-based, using traditional backup agents that coordinate backup by looking at the files from the Host side.
- NAS – Fiber Channel, the backup system communicates directly to the array instead of the host to take the backup.

Specific process documents are discussed in the table below.

Process Documents

PROCESS	PURPOSE
HPE Data Protector Backup Verification Process	This purpose of this document is to verify that backup data can be restored and read. This shall be performed weekly by the BUR Administrator.
Preparing HPE Data Protector Cell Managers Prior to Scheduled Backups	The purpose of this document is to outline the steps preparing HPE Data Protector Cell Managers prior to scheduled backups. This shall be performed weekly by the BUR Administrator.
Upgrading the DPA Collector Agent on HPE Data Protector Cell Managers	The purpose of this document is to outline the steps to upgrade the DPA collector agent on the HPE Data Protector cell manager servers. This shall be performed weekly by the BUR Administrator.
Restarting Stalled or Unresponsive HPE Data Protector Backup Sessions (DOC ID BUR 0010)	The purpose of this document is to provide the process to be followed when In-progress backup sessions appear under Monitor in the HPE Data Protector Manager GUI, but attempts to view the

PROCESS	PURPOSE
	session result in the GUI freezing. This shall be performed as needed by the BUR Administrator.
StoreOnce Troubleshooting (DOC ID 0015)	Outline the process steps on how to troubleshoot the StoreOnce application. This shall be performed as needed by the BUR administrator
Workaround for Hung Sessions Due to Catalyst Media Server Timeout (DOC ID 0017)	Outline the steps and workaround procedures for hung sessions due to Catalyst media server timeouts. This shall be performed as needed by the BUR administrator.
How to Restart and Resume County of San Diego Backup Sessions (DOC ID 0018)	Outline the steps for restart and resume County backup sessions once failed objects and sessions have completely failed. This shall be performed as needed by the BUR administrator.
How to Kill the HPDP Session Using PID with Catalyst Devices (DOC ID 0019)	The purpose of this document is to outline the process steps on how kill the HPDP session using PID with Catalyst devices. This shall be performed as needed by the BUR administrator.
How to Archive Bit Reset Configuration for SQL Flat Files in HPE Data Protector (DOC ID: 0020)	Outline the process steps on how to archive bit reset configuration for SQL flat files in HPE Data Protector. This shall be performed weekly by the BUR administrator.
Resolving Latency on User and Data Shares (DOC ID: 0021)	Outline the steps and procedures for resolving latency on End-User and data shares. This shall be performed weekly by the BUR administrator.

Integration of data with Backup and Recovery Services, using required connectors such as Oracle RMAN and VSS.

Contractor shall support and maintain RMAN to write database backup files to spinning storage that is made available on the database server for the purpose of backups. The cost of the licenses for Oracle RMAN is not included in base services. The backup files on spinning disk shall then be captured in the next Contractor Data Protector backup. The files shall be stored on Contractor's tapeless backup media and replicated over a dedicated replication network connection to the DR site hundreds of miles away in Colorado Springs. Contractor shall support the creation of VSS (shadow copies), and the Contractor backup solution shall also be able to back up VSS shadow copies directly with a local copy of that backup written to the tapeless backup target and be replicated to Contractor's remote backup media.

6.14. Managed Print Services

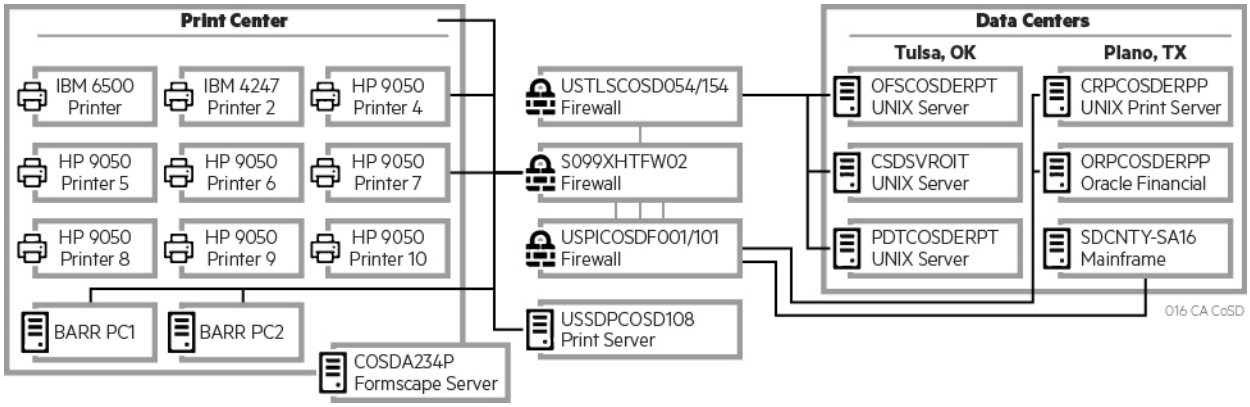
6.14.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall provide managed print services via the County print room facilities located at the Rancho Bernardo site. Contractor's print operations processing shall take place Sunday through Friday from 8:30 p.m. to 2:00 p.m. PT, with on-call support available as needed.

With the transition of the Juris-managed print requirements to Fujitsu, Contractor shall continue to provide managed print services of approximately 200,000 pages per month on average to meet Assessor and Tax Collector requirements. This shall be conducted at Contractor's print facilities at the Rancho Bernardo site. Contractor shall use the BARR print management tool to receive the files for printing. **Error! Reference source not found.**The figure below illustrates how print files are currently transmitted to Contractor's print center.

Transmission of Print Files to Required Printers



Migration from SA16 LPAR Mainframe to the Integrated Property Tax System (IPTS) shall consolidate and modernize the legacy property tax systems in a web-based system designed to vastly improve the efficiency of the property tax-collecting process. It shall also generate the tax bill files for printing. After implementation of IPTS, Contractor shall update processes and procedures associated with running daily print jobs for County Assessors and Tax Collectors.

Contractor shall provide the following services for the managed print framework component:

- Order supplies such as Contractor print toner and printer maintenance kits
- Ordering special forms and paper
- Provide support for microfiche

- Daily delivery of reports Deployment plan for resources and use of facilities

Contractor's primary print facility shall be the Contractor's Rancho Bernardo site and with the implementation of a disaster recovery solution, multiple geographically diverse sites shall have the capability to provide print services for the County. Print jobs shall be easily routed to any location. **Error! Reference source not found.**The table below summarizes the specific types of printing provided at each location.

Types Printing Provided at Each Location by Contractor

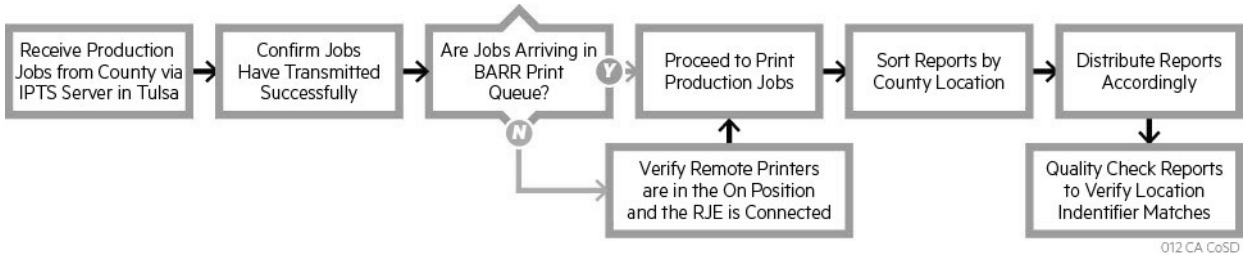
TYPE OF PRINTING	LOCATION
Laser and Impact Print	Rancho Bernardo
Annual tax bills, supplemental (small volume) tax bills, and tax bills that require manual intervention of the Treasurer-Tax Collector's (TTC) office.	Rancho Bernardo, with backup at Rancho Cordova
One-stop document and tax bill management—folding, envelope stuffing, and mailing	Rancho Cordova
Laser Print and Tax Bills (Dev/Test)	Troy, Michigan (trial) Rancho Bernardo Rancho Cordova

Contractor's dedicated staff shall work in the print center at the Rancho Bernardo site with responsibility for printing, distribution, and delivery of daily work.

- Key methodologies and processes in solution including year-to-year continuous improvement

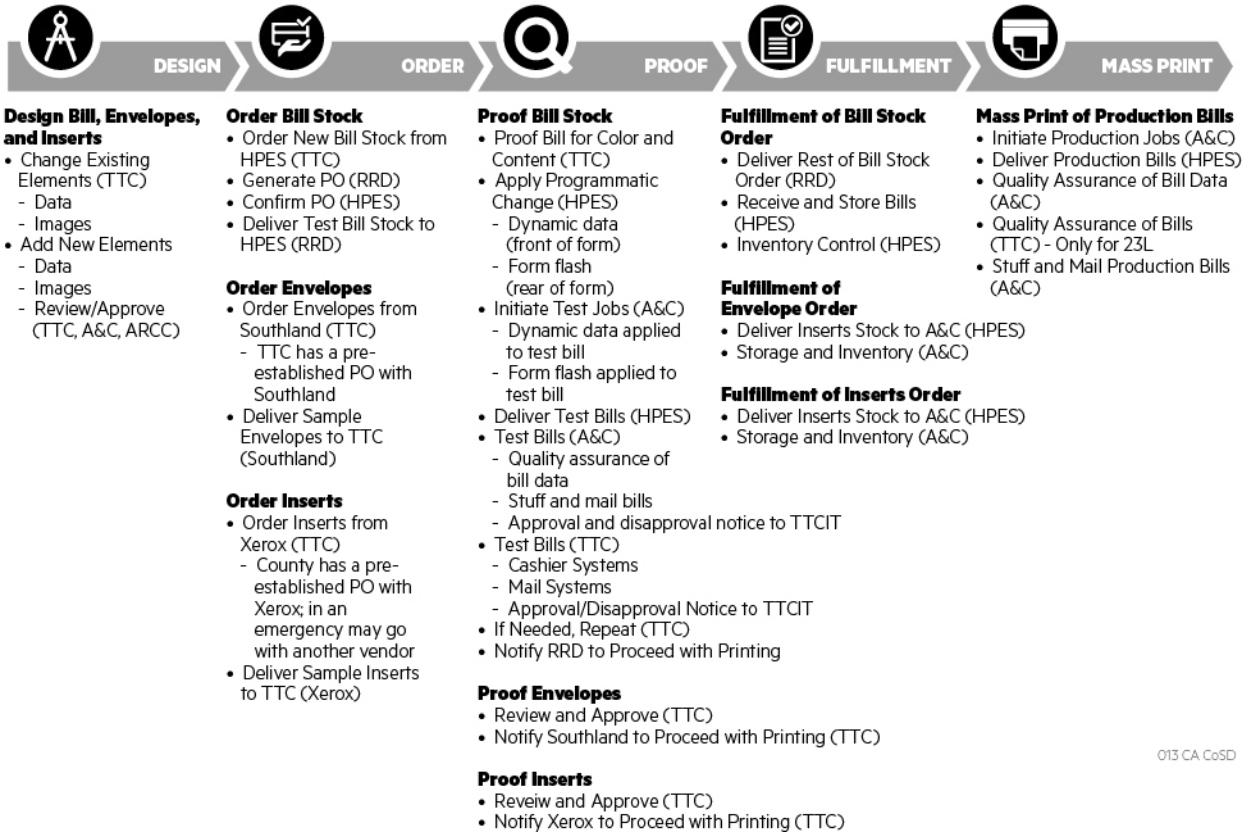
The figure below illustrates the process Contractor shall follow to receive print requests and print the reports for distribution to the County within the prescribed timeframe in Service Levels.

Contractor Process for Receiving and Printing Reports



Contractor shall follow the process checklist shown in the figure below and documented in the Standards and Procedures Manual.

Tax Bill Generation Process



Contractor shall use the BARR Systems Print Server to automate and control print and document output.

6.15. Public Key Infrastructure (PKI) Services

6.15.1. Process and Procedures

- Description of solution to meet the requirements

Contractor shall leverage the current MPKI 8.13 solution and use that as the foundation for additional PKI services. This solution shall be a fully extensible and redundant platform sized for the current project as well as future functionality. Key features and benefits of the Managed Symantec PKI solution shall be:

Key Features

- **Trusted, Cloud-Based Infrastructure:** Monitors, manages, and escalates across the globe with full DR and is certified as part of a SAS-70 security, WebTrust and specialized Government audits.
- **Broad Application Support:** Issuance of X.509 certificates that interoperate with operating systems, devices, VPN, mail, and web browser software. Certificate profiles for common applications are for email encryption and signing, and Adobe PDF signing.
- **Automated Certificate Life Cycle Management:** Automates configuration of authentication, encryption, and signing applications across platforms and browsers. Managed PKI service can automatically configure an End-User's browser, VPN client, mail client, or other application to use certificates. PKI Client also automates renewing certificates and prevents expired certificates from interrupting business continuity.

- **Enterprise Integration:** Integrate Managed PKI Service with a corporate directory to populate certificate meta-data, select and enforce certificate and application policies, and publish issued certificates. PKI Enterprise Gateway functions as a local registration authority integrating with hardware security modules to protect key material.

Key Benefits

- **Reduces PKI Cost and Complexity:** Managed PKI service's cloud-based approach dramatically lowers cost and complexity by eliminating the facilities, hardware, software, personnel, training, and maintenance expenses associated with deploying traditional in-house PKIs.
- **Simplifies the Administrator and End-User Experience:** Eliminates administrator tasks, and automates the process of provisioning certificates and configuring applications to use those certificates.
- **Maximizes Deployment Flexibility:** Not only can organizations deliver multiple certificate-based security applications from a unified platform, but they can also tailor the deployment to meet their needs.
- **Delivers Proven, Scalable, Reliable PKI:** Symantec's procedures, policies, and infrastructure have been proven with large enterprises, governments, and manufacturers around the world

Self-service via the Service Portal shall be made available for specific use cases, for optional services or functions, such as certificates required for digital signing of expense reports.

The approved County solution for digital signing is the existing ARX/CoSign document. Contractor shall work with ARX/CoSign to develop and implement previously identified changes in the document signing solution to utilize the Symantec PKI certificates as part of transition.

Contractor shall integrate Symantec PKI with DocuSign CoSign. Currently the internal CoSign CA is used to generate and revoke certificates. This shall be replaced by a web service invocation to Symantec Cloud-based PKI. Today the enrollment process automatically occurs when a County End-User on a County machine attempts to sign a document or open any application that uses the CoSign client plugin (e.g., Word, Excel, Adobe Reader/Acrobat). This process shall remain unchanged. During the enrollment process, the CoSign appliances shall invoke a web service against the Symantec Cloud-based PKI to fulfill the certificate creation request. Once complete, the private key of the certificate shall be stored in the appliances' internal store (as is done today). Subsequent requests to sign documents shall be fulfilled by the appliances only with no need to invoke Symantec services. This approach has already been successfully developed and deployed between CoSign and Comodo with production use by a number of customers. In addition to firmware changes, CoSign shall have to recertify their appliances if Federal Information Processing Standard (FIPS) compliance is required. Firewall rule changes at the County shall need to be created to allow connectivity between the appliances (currently in the data center zone) and Symantec PKI cloud. No changes are anticipated for Symantec. Additionally, no changes should be required for the CoSign clients residing on County desktops/laptops.

Contractor shall support the PKI solution using a combination of Contractor local resources and Contractor leveraged resources as part of the Identity Access Management solution. The PKI shall be supported per the Data Center support model as stated in Infrastructure Services. PKI functionality shall be supported by the local Security team and the Contractor Identity Access Management team, which shall support Active Directory and ADFS as well as other AD integrated solutions. Operational support functions shall include monitoring certificate status to identify when they are to be revoked or renewed as well as administrative management of certificate profiles and users.

- Deployment plan for resources and use of facilities

Contractor staff shall be located at the following sites to support the County:

- Rancho Bernardo. Primary location of dedicated Contractor staff specifically assigned to support the County. It includes centralized meeting space for engagements between the County and its contractors and Contractor

personnel, including security staff and Contractor executives, and is the initial point of contact for the County. Test environments, training, and video conferencing are also housed at this site.

- Contractor Tulsa Data Center. This is the core data center that shall house the majority of the County IT infrastructure and delivery of core IT services as well as security services.

Certificate Practice Statements (CPS) state the terms and conditions associated with certificate use between County and external entities and typically come into play into the event of perceived misuse. The County needs to complete the CPS, and Contractor shall facilitate that process.

7. APPLICATIONS SERVICES

7.2. Application Maintenance and Operations Services

- Deployment plan for resources and use of facilities

Contractor shall utilize Contractor's Rancho Bernardo office, County locations as requested/required, and application development centers in El Paso, TX and Pontiac, MI.

7.2.1.1. Process and Procedures

Applications Maintenance & Operations (M&O) Services

Contractor shall provide a bundled approach. Applications shall be bundled based on level of service appropriate to each bundle. On a quarterly basis, or as requested by the County, Contractor shall review the application portfolio with the County to determine growth or reduction of applications and determine if a bundle adjustment is required. As a part of the review, Contractor and County shall establish an Application Review Board (ARB) to evaluate the activity and provide "move forward" recommendations. The ARB shall consist of County representatives and Contractor representatives, as further detailed in the Standards and Procedures Manual. The Application Review Board, with participants determined by County CIO and Contractor AE, shall review all impacted billing low-orgs to determine if growth or reduction adjustments are required to either one or more Applications M&O FFP bundles or the FFP Dev/Test RU. Annual pricing reductions to the FFP M&O shall be 2% beginning Contract Year 2.

The applications are separated by bundles types into three groups—(full support, coordinated support, and Software as a Service (SaaS) support) across the five business areas.

	Concept Considerations	**Concept Considerations**
By County	3 RUs (one for each bundle type)	Allocation to be determined/executed by County
By Business Group	15 RUs	Further allocation would be determined/executed by the County.
By Low Org	131 RUs	Assumes 47 depts., some may not have all 3 RUs. Low-org may be a better grouping as some departments often uses a single low-org regardless of department or division.

Applications M&O Services shall include all services (e.g., labor), software, hardware, and required system environments. For example, Contractor is responsible to provide Break/Fix environments to support an application (e.g., to test new patches or versions), that is included in the FFP Apps M&O RU, and FFP Dev/Test RU.

High Level Key Benefits to the FFP Apps M&O

- Predictability of costs
  - One monthly charge (by County, Group or Low-org)
  - Discount offered by Group or by County options
- Predictability of budgeting
- Cost reduction Year-Over-Year beginning CY3
- All PA-IDs are covered
- Maintenance of applications are more timely
  - Not reliant on additional department funding for standard/routine application patches and updates (including 3rd party)
- No limit to skillset utilized to resolve issues
  - Eliminating the dispute when a break-fix incident requires an architect or engineer yet the NDSR does not support that skill
- Contractor assumes the risk of increasing costs

The priority levels assigned to all Portfolio Applications as of the Contract Effective Date (CED) shall remain the same for the Term of the Agreement unless otherwise agreed upon by the parties in accordance with the Agreement.

- Solution to meet the requirements

Contractor's solution shall include the transition of all of the County's Applications M&O (M&O) activities to the FFP model. In Contractor's discussion below of 10 high-level M&O requirements that follow, Contractor shall distinguish between Applications M&O activities and Application development activities.

Contractor shall develop process improvements automation to reduce the cost of M&O services over time. All application patches for routine maintenance and/or restoration of services shall include UAT.

Contractor has assembled the County applications into 3 options/bundles where each option may have 3 support models full support, coordinated support and cloud-based Software as a Service (SaaS) support.

	Concept Considerations	**Concept Considerations**
By County	3 RUs (one for each bundle type)	Allocation to be determined/executed by County
By Business Group	15 RUs	Further allocation would be determined/executed by the County.

By Low Org	131 RUs	Assumes 47 depts., some may not have all 3 RUs. Low-org may be better grouping as some departments often uses a single low-or regardless of department or division.

Full support comprises a full range of application activities from Break-Fix incidents response, restoration of service, M&O activities such as installation of patch/upgrades for routine maintenance activities. Full support includes those applications where Contractor has the access and ability to affect change either with or without the participation of a third-party vendor.

Coordinated support applies to applications where Contractor hosts the application but does not have security access or the ability to affect change. Contractor shall engage with the vendor and coordinate the necessary change(s). When possible**,** provided by 3rd party and approved by the County, M&O activities such as coordination of Break-Fix incidents response, restoration of service, installation of patch/upgrades for routine maintenance activities shall be performed.

SaaS Support are cloud-based applications where Contractor does not host the application and has no ability to affect a change. Contractor shall contact the SaaS provider and keep the County informed of the status of the issue or change.

On a quarterly basis, the ARB shall review the Applications Portfolio to evaluate the number of applications that have been added or retired and determine whether the RU warrants adjustment. This review shall also occur upon County request or in the event Contractor identifies a material change, as that term is defined below.

Material changes are additions or deletions of Portfolio Applications that affect the M&O support or server environment and that meet any of the following criteria:

1. Fifty (50) or more End-Users
2. Adding or deleting five (5) or more servers to Dev/Test
3. Adding or removing an app representing >30% of a billing low-org

As needed upon recommendation of the ARB, the County CIO and Contractor AE shall review all impacted billing low-orgs to determine if growth or reduction adjustments are required to either one or more Applications FFP bundles or the FFP Dev/Test RU.

Unless modified by a Service Request, Portfolio Applications shall be added into the appropriate FFP M&O bundle immediately upon implementation into production or upon the expiration of a stated warranty period, whichever is later.

For addition of a large application (e.g. ConnectWellSD) or a complex enhancement to an existing application (e.g. adding Open Enrollment to PeopleSoft), which requires 1500 hours or more of labor, the County shall deliver a Service Request to Contractor to perform M&O activities for up to six (6) months as time and materials. During this time, Contractor shall provide a report of M&O support, "actuals," and a detailed report of hours and tasks performed to determine the future adjustment to the appropriate FFP bundle. The ARB shall review the report of the six (6) month sampling for reasonableness and shall then provide a recommendation to the County CIO and Contractor AE.

Restore Service Levels

First, Contractor shall validate the restoration requirements for each application and structure Contractor's team to meet those requirements. If an application requires 24x7 onsite support for restoration of services, Contractor shall staff and schedule the response team to be sure M&O staff is available 24x7. If an application requires 24x7 on-call support, Contractor shall schedule staff to be standing by to respond to an outage 24x7. Applications that require less than 24x7 shall be supported in accordance with priority to specific County business needs. Contractor shall provide a Monday through Friday, 6:00 a.m. – 6:00 p.m. support window for all other applications;

Contractor shall build and enhance applications to prevent outages. As part of application portfolio maintenance, Contractor shall design and develop applications to be hardened and not fail. Contractor shall evaluate the supporting software middleware, and hardware for the application to verify the application's supporting components deliver required Service Levels without disruption. Contractor's team shall thoroughly test the application's new functionality, regression test unchanged functionality, and performance test the application executing simulations in a Dev/Test environment before implementing a change.

Contractor shall operate to restore applications functions as quickly as possible in the case of outage, whether application or infrastructure based. Contractor shall follow the Incident Management process detailed in, Cross Functional Services. Technical support shall triage as soon as they are notified by the Service Desk, and work the issue until functionality is restored. For mission-critical outages, the support staff shall use additional SMEs as needed and reach back to vendors and suppliers when necessary to resolve the outage. The Service Desk, with information from the technical support staff, shall notify Contractor management of the outage, and Contractor management shall notify County management.

When a change to the application is required to resolve the outage, Contractor shall perform the necessary application changes, data updates, and/or third-party software patching, to restore services in accordance with County emergency fix process. All application patches for routine maintenance and/or restoration of services shall include End-User acceptance testing, as desired by the County.

Contractor's application services team shall build new applications and enhance existing ones to prevent outages. Contractor shall make recommendations for changes to applications, and perform monthly analysis to identify defect rates, annual cost, and technical obsolescence within applications. As part of the ARB, Contractor staff shall work closely with the County board representatives and present outage incidents, provide recommendations regarding technical obsolescence, and review portfolio additions and deletions. A standard agenda shall be developed and reviewed at each meeting.

Production portfolio applications maintenance

Contractor's plan to maintain the portfolio focuses on keeping production up and running with a goal of no disruption to the County. In addition, Contractor shall continually improve applications to optimize performance and apply patches from third-parties.

Contractor shall make maintenance changes to production applications upon a County-approved request for change (RFC). Contractor shall meet weekly with the County to review the pool of RFCs and determine the priority and whether it can be approved for implementation. Contractor shall schedule the implementation of approved RFCs based on County priorities and approval.

When Contractor implements an RFC to fix a bug, install a patch, or implement an upgrade as part of M&O, Contractor shall follow Contractor's existing SDLC methodologies and the County's change and release management processes. Contractor shall functionally test RFC implementations and perform regression and performance tests. While implementing the change, Contractor shall build in warnings, notifications, and processes to provide application support of the RFC during operations if needed.

In conjunction with the County, Contractor shall define the authorization requirements (security) for End-Users, roles, and schemas and shall provide provisioning and de-provisioning of End-User and service accounts for the portfolio applications as authorized.

If a firewall change is required by M&O activity, it is covered under Apps M&O. If the firewall change is required by a new application or new End-User request (adding DA or hospital access), it shall be costed as part of the project.

With every service restoration fix, patch, or minor maintenance implementation, Contractor shall update the appropriate portfolio application documentation in accordance with the new functionality in production and all application document artifacts impacted by the RFC, including application document libraries, configuration management databases, and application management system, known as AppsManager.

Contractor shall evaluate the applications architecture, configuration, and system upgrades and identify opportunities for improvement. When opportunities are identified, Contractor's team shall initiate new RFCs and implement them after approval by the County.

In addition to implementing changes, Contractor's team shall support the application in production. Contractor shall build an application support team with the right number of staff with the right skills set and expertise to support the applications in production. RFCs are implemented in adherence to Contractor's SDLC process, the County's change management and release management procedures, and County governance approvals. Contractor shall provide services based on ITIL-aligned processes, CMMI standards, and other leading practices as appropriate. Contractor's project managers and applications subject matter experts (SMEs) shall work with the County and its delivery and application product owners to build a project plan to provide predictable, repeatable, and successful results.

Contractor's M&O services team shall provide planning, monitoring, and schedules for new applications as they are placed into production. The team shall respond to warnings and notifications generated by the applications and fix the issue that triggered the warning or notification. Contractor's infrastructure support team shall monitor the operating environment supporting the applications. Contractor shall triage application and hardware incidents and take the appropriate action to restore service.

Contractor shall execute End-User administration for the applications following the application's processes and procedures for End-User administration, including the necessary County approvals. Contractor shall update the appropriate portfolio application specific documentation as necessary, as well as Service Desk scripts, application data elements in AppsManager, and the Service Portal.

Contractor shall perform periodic reviews that may result in recommendations for application security improvements, product and software changes, or improved performance and cost savings. Contractor shall provide recommendations to County business owners and CTO to make sure the performance of the applications portfolio is optimal.

As part of M&O activities, Contractor's staff shall perform special testing for events such as public holidays, end of financial year, end of calendar year, and daylight savings time.

Application M&O Scope

M&O activities shall include executing the process to maintain application interfaces and coordinating with third parties to manage those interfaces. M&O includes performing the necessary preventive maintenance, routine system patching, application upgrades and code releases, but only as required for restoration of services, mitigation of security vulnerabilities, and implementation of a maintenance release. Notwithstanding the foregoing, if a routine system patch, restoration of service patch, or

application upgrade includes an Enhancement, as that term is defined below, the implementation of which exceeds reasonable Contractor work effort, Contractor shall have the option to escalate the review of cost allocation to the ARB.

An Enhancement is defined as any product change or upgrade that increases software or capabilities beyond original specifications. It can also be distinguished as an improvement (enhancement) of an existing application capability or a totally new capability.

Applications M&O shall not include County requested Enhancements (including security Enhancements) or County requested application upgrades (e.g. PeopleSoft 9.2 upgrade or SharePoint 2013 upgrade).

In the event of a service outage resulting from application or infrastructure abnormalities, Contractor's M&O staff shall perform necessary code fixes to restore service in accordance with the bundled service. The SDM shall drive incident management activities and provide ongoing communication to the client. As a result of the service restoration, Contractor shall execute the necessary root cause analysis (RCA) to investigate the outage issue, following the RCA process as described in Cross Functional Services. These activities shall include analysis, design, coding, testing, data conversion, documentation, End-User coordination and communication, and production turnover activities and the management of these activities for restoration of service. Based on the RCA findings, Contractor shall recommend modifications to the application to prevent future outages, including those attributable to a Third Party.

Align Maintenance Activities with County architecture standards, guiding principles, and architecture bricks and patterns

All Architecture activities required by Apps M&O shall be included in the Applications M&O RU. Contractor's shall align with County IT architecture standards while participating in the process to improve, refine and enhance them. Contractor shall monitor technology trends, best practices, and products within the IT industry, recommend enhancing County processes when appropriate, and Contractor shall provide a repository to document and manage standards, available through the Service Portal. Contractor shall build any additions into standard processes and practices.

On an agreed to schedule, Contractor shall participate in annual technical and business planning sessions, including bricks, to enhance standards, architecture, and project initiatives.

Contractor shall perform maintenance activities following the Standards and Procedures Manual as updates occur and shall implement all modifications to make sure Contractor's staff is aware and trained.

Provide M&O services for portfolio applications in production environments including servicing middleware and other application supporting components.

Contractor shall maintain both nonproduction and production environments for applications. This maintenance shall include keeping non-production configurations synchronized with production. Contractor's M&O staff shall keep the application and its supporting components, such as middleware, synchronized. Contractor shall accomplish this by updating supporting components using the same processes Contractor uses to update the applications. Contractor's M&O staff shall initiate an RFC to update components and implement the update when approved and scheduled by the County.

Contractor shall put steps in every project schedule to update the non-production environments with any approved component upgrade.

Maintain accurate and continuous prompt updates to asset and system documentation

Each approved Request for Change (RFC) shall include a step to update application documentation. This shall include updating asset and system documentation and tools. M&O staff shall be responsible for the technical accuracy and specific details of the update, and staff leads shall review the changes for accuracy and completeness.

Validate cross-framework integration and communication is conducted for application incidents, outages, maintenance work, planning purposes and all changes

Contractor shall validate cross-framework integration by regression testing application bug fixes and enhancements prior to production implementation. Contractor shall build and maintain test (Break/Fix) environments that include or simulate cross-framework integration, and Contractor shall build Contractor's test plans to include cases to test the frameworks.

Contractor shall keep County stakeholders informed on the full range of application activities from incidents, M&O activities, and changes.

The applications team shall follow the outage management communication process.

Provide services in alignment with ITIL and CMMI standards to ensure predictable, repeatable, and successful results

Contractor shall use industry best practices to enhance effective planning, execution, tracking, and delivery of services to the County. Contractor's repository shall provide the backbone of Contractor's process improvements and includes templates, guidelines, checklists, and lessons learned. It complies with recognized industry standards, including the Project Management Institute's (PMI) Guide to the PMBOK, ITIL, International Organization for Standardization (ISO) standards, and the practices incorporated in CMMI Institute's Capability Maturity Model Integration (CMMI).

Implement new patches and versions (within the current release), prioritizing patches that address security vulnerabilities

Contractor shall implement new patches and versions under M&O following the existing RFC process. Contractor shall create a plan to communicate, test, and implement each patch or version. All patches and versions shall be discussed with the County business owner and CTO to determine criticality, scope of change, priority, and timing. Following successful testing, Contractor shall submit an RFC for approval and scheduling.

When competing patches are released, patches that address security vulnerabilities shall get priority, along with those that fix critical issues. Next priority shall be patches that address minor issues, those which have a workaround available, and lastly patches that address issues that have not impacted County users.

Perform Maintenance Services that include Preventive, Adaptive, and Perfective Maintenance

Contractor shall perform application maintenance as part of M&O service. Contractor understands the objectives of preventive, adaptive, and perfective maintenance with respect to M&O to be as follows:

- **Preventive Maintenance** – Maintain application reliability to prevent issues from emerging in the future
- **Adaptive Maintenance** – Modify the system to adapt to changes in the business environment.
- **Perfective Maintenance** – Modifications and updates to sustain application usability and improve its reliability and performance.

Contractor shall perform preventive maintenance to resolve known problems and defects; perfective maintenance to optimize and tune performance; and adaptive maintenance to remediate impacts resulting from interfacing application changes, changes to application middleware, or changes to the infrastructure.

- Processes in solution including year-to-year continual improvement.

Contractor shall use County-approved procedures and standardized industry processes and governance based on PMBOK, ITIL, and CMMI as well as the Contractor operations excellence support methodology and repository of best practices and lessons learned. By driving the adoption of standards, taking full advantage of developments in technology, and being flexible and agile, Contractor shall help the County transform and manage its environment to achieve a balance of maintenance and innovation, reliability, and change. These methodologies shall enable Contractor's team to prevent outages and defects before they occur by thorough testing during the development phase. In the event of an incident, however, Contractor's methodology provides responsive M&O for fast and effective resolution.

For continual improvement, Contractor shall regularly review incident reports, RCAs, and application performance data so that applications are optimized appropriately. Contractor shall also monitor industry best practices as well as emerging trends and new technologies to determine if a different solution provides a better outcome. All this information shall be shared and reviewed with the CTO.

Contractor shall develop process improvements and automation to reduce the cost of the M&O services.

Process used to migrate developed Applications into (and retire/decommission Applications from) the Applications Portfolio, including the approach, data requirements, timeframes, and analytic approaches to ensure a reasonable fixed price for Applications M&O Services.

Throughout the year, applications are added and retired from the Applications Portfolio. The County initiates additions and retirements as an approved request.

When adding an application to the M&O portfolio, unless otherwise requested by the County through a Service Request, Portfolio Applications shall be added into the appropriate FFP M&O bundle immediately upon implementation into production or the expiration of a stated warranty period, whichever is later.

Addition includes updated Service Desk scripts and entry of application details into the AppsManager tool. Support for the application shall be part of the FFP M&O.

For addition of a large, complex such as Connect Well San Diego or implementation of an additional module to an existing app, a service request shall be delivered to Contractor to perform M&O activities for up to 6 months.

Large, Complex is defined as a Portfolio Application modification estimated at 1500 or more total labor hours.

During this time Contractor shall gather and report M&O support 'actuals' to determine the future adjustment to the appropriate FFP Bundle.

Conversely, if an application is to be removed (retired) from the M&O portfolio, the M&O team shall perform all functions required to retire that application, including decommissioning the infrastructure and updating Service Desk scripts. Applications shall be retired by the direction of the County using a non-billable Service Request.

Contractor shall develop process improvements and automation to reduce the cost of the M&O services.

Third-Party Software packages are updated to current versions. Frequency with which Contractor's organization typically implements upgrades. The process Contractor undertakes from initial testing through production implementation and the value added by this process. Describe the process which shall be followed to keep County representatives aware of the availability of Third-Party Software package upgrades.

Approach. Contractor shall catalog and track all third-party software used by the County to make certain that software is maintained to the current versions. Contractor shall report to the County application primary contact on third-party software with upcoming updates. Contractor shall meet with the County and shall recommend third-party software upgrades. All changes shall follow Change Control Review Board (CCRB) in accordance with County processes and procedures for third-party software.

Frequency. Contractor shall proactively track upcoming updates to third-party software through the Internet, direct contact of third parties, and/or by announced vendor notices or technical updates. Upgrade frequency to third-party software shall depend on the software vendor and County direction.

When patches or upgrades are published for release, Contractor shall notify the County application primary contact that a release exists. Upon approval of the County CCRB, Contractor shall initiate the process for upgrading third-party software as outlined below.

Contractor shall conduct weekly meetings between Contractor and the County CCRB in which decisions on upgrades are addressed. If greater frequency is required, Contractor may request on a case-by-case basis an emergency meeting of the County CCRB specific to any urgent upgrades that Contractor believes require immediate County attention and approval (for example, patches that remediate security vulnerabilities).

Process — Testing Through Implementation. Once Contractor receives an upgrade, Contractor shall stage that upgrade and run tests in accordance with Contractor's Standard Procedures.

Initial testing shall start with the development of a testing plan and installation of the patch release/upgrade in a testing environment. Staff from Contractor and the County shall test the new version of the third-party software.

User acceptance testing (UAT) may include specific testing scripts and scenarios, depending on the application and the amount of enhancement. Once UAT is completed, results shall be presented to the County for approval and signoff.

Upon UAT approval, Contractor shall schedule and prepare for software installation into the production environment. This process shall be consistent with existing County processes and lends itself to a predictable, reliable, and controlled approach for upgrading third-party software for the County.

Upgrade Availability Communication. Contractor shall meet weekly with the CCRB to review the recommended changes. Each proposed change shall be approved by the County CCRB and the County representative. At such time that the proposed change is approved, Contractor shall schedule the change to accommodate the application downtime window.

Applications Services Framework

- Use of Tools

Contractor shall provide automation tools such as Contractor's APM which provides a 360-degree view that verifies the performance of desktop, web, and mobile apps for on premise, cloud, or hybrid environments, as well as Cascade, SCCM, and various other network related tools

- The implementation of APM shall enhance Contractor's ability to:
- Provide end-to-end visibility of transactions including back-end systems and mainframes
- Monitor the End-User application experience and services
- Quickly find and resolve application performance issues
- Collaborate with application development teams to effectively resolve application and transaction issues
- Reduce mean time to repair critical business transactions
- Monitor performance of applications deployed to a cloud or virtual environment
- View application performance alerts anytime, anywhere on the End-User's mobile device.

Contractor shall provide and use Cascade, SCCM, HPE Operations Manager, and other network and system related tools and reports to identify and correct issues in the environment related to applications, desktops, web, mobile applications, and others. The addition of APM shall assist to close the circle of the end-to-end reporting so that Contractor can be proactive in addressing systemic issues and making sure Contractor's solutions are running as expected to support the applications.

The SDMs shall work with the application SMEs, vendors, and the Enterprise Problem Manager to make sure that any and all items identified through these tools and reports are being acted on quickly to reduce the amount of impact to the End-Users as described in Service Delivery Management and Problem Management Services.

Contractor shall provide Project and Portfolio Management (HPE PPM) module for consolidating, prioritizing, and fulfilling application services activities and development projects so the County has visibility into all of the demands on the infrastructure. Its web-based dashboards provide real-time visibility into request status, priority, next steps, and summary views. Service levels are updated automatically as each request is processed.

Contractor shall provide a Service Portal that shall automate Service Desk ticketing, for incident and break/fix resolution.

On an ongoing basis, Contractor shall evaluate additional tools to further automate M&O activities, such as self-healing tools and discuss any recommendations with the County.

- Alternate Time & Materials model to provide Applications Maintenance and Operations services

Time and Materials (T&M) or Non-Discretionary Service Requests NDSR-like ("NDSR") Process

NDSR Rules of Engagement:

- All applications shall have an NDSR
- NDSRs shall be by PAID, Low-org, Department or Group
- Funding amounts shall be established for the County fiscal year
    - Invoicing shall be monthly based on actuals
    - If utilization reaches 80%, Contractor shall notify the County
    - If utilization reaches 90%, Contractor shall submit a Change Request to increase funding*
        - Regardless of available funding, all T&M activities shall be billed to the Low-Org associated with the corresponding NDSR (in the event the change request is not approved in time to cover a break-fix activity)

  - Contractor shall provide estimates (based on actuals) to assist in establishing appropriate NDSR funds on a monthly basis to forecast trending
- NDSRs cannot limit the job classification approved to work on a break-fix
  - Charges to the County are task-based, not person-based

Note: If a NDSR requires chronic changes (meaning the County user set the funding intentionally low, thereby requiring change requests on a regular basis to replenish the funding), Contractor shall notify the County CIO for resolution.

7.2.4. Application Programming

7.2.4.1. Process and Procedures

Application Programming

Application programming are those activities associated with the programming, scripting, and configuring of application modules to support M&O activities.

Contractor shall perform applications programming using and adhering to the County's technical and architectural standards as well as standards and procedures, performing all necessary steps to complete M&O tasks. Contractor shall use Microsoft Team Foundation Server (TFS) to create working directories and store source code.

7.2.5. Application Integration and Testing

7.2.5.1. Process and Procedures

Application integration and testing shall be services that confirm the individual application framework components work together properly and, as a whole, perform its specified functions.

Contractor shall plan and develop Contractor's testing procedures to meet County requirements and policies. Contractor shall document the testing procedures in the Standards and Procedures Manual, including procedures to be followed by an independent testing team as needed. Contractor shall develop an overall test plan for M&O releases that includes the test strategy, coverage, scenarios, test bed, test data, methods, schedule, and responsibilities.

Contractor shall build and maintain an application testing environment that has been refreshed with production data. If necessary, Contractor shall build data masking programs to disguise production data. Contractor shall build test cases to test the new functionality or components based on the requirements and determine which valid data is required to appropriately test the application as well as the various testing phases. Contractor shall create a set of test cases to test the application end-to-end, new and existing functionality, application security and application supporting components, and infrastructure, when needed, to support M&O activities. Benchmark test cases shall also be created and run to properly execute regression testing. Contractor shall provide a reference to link requirements and test cases.

Contractor shall execute the test cases while following the standard testing procedures and verify that the results meet County testing requirements. Contractor shall track defects in a County-approved tracking

tool and shall correct retests functionality to validate repairs. In addition to testing the application, Contractor shall provide an UAT environment, if needed, it shall include the necessary data. Contractor shall provide support to the County in its UAT testing effort and provides access to the defect tool for entering found defects. Contractor shall assess and report potential risks to production of implementing a change and only implement after County approval.

Contractor shall manage the various testing environments including the application data, application releases, and supporting software and components. Contractor shall stage the applications changes in the appropriate system in preparation for production implementation. Contractor shall provide support to these implementations, track their migration status, and verify the implementation of changes into production. Contractor shall define the test-to-production turnover requirements and instructions for each project or release and report the results, which shall be shared with the County.

7.2.6. Application Implementation and Data Migration

7.2.6.1. Process and Procedures

Application integration and testing for M&O activities shall be defined as those activities associated with the installation and migration of new patches and maintenance upgraded components to the production environment.

Contractor shall create a detailed plan for each M&O release. Contractor shall have a "go/no-go" checklist, after approval of UAT. All M&O releases shall include rollback steps and, Contractor shall update any affected application documentation and production application support documents and procedures as needed.

Contractor shall execute, coordinate, and communicate with the County for all releases and associated activities. For each patch and/or upgrade, Contractor shall perform the needed steps of the SDLC such as requirements analysis, design, development, and testing as appropriate for M&O activities. Contractor's deployments shall follow the County's change and release management processes and are compliant with client change management policies. Documentation shall be regularly updated, including the Standards and Procedures Manual and Service Desk scripts. Contractor shall execute the deployment in production once approved by the County and Contractor shall synchronize the production and non-production environments.

7.2.7. Application Documentation

7.2.7.1. Process and Procedures

Application documentation is defined as the development and maintenance of documentation for all applications. Contractor shall continually improve application documentations, providing new and updated documentation when required for system specifications, technical documentation, operational processing flows, system installation, application production support manuals, configuration plans, tuning instructions, release notes, and solution design as needed for M&O upgrades and patches. Contractor shall execute application updates as needed with every release, including patch and update releases as defined in "Production portfolio applications maintenance".

Contractor shall build and maintain documentation folders for each application, which shall be stored online with County controlled End-User access. All documentation created or updated for a release shall be stored in the folder in DocVault and shall be updated at the same time as the release implementation.

This shall help to keep the documentation in sync. Contractor shall store updated code and application components in the code CMDB to maintain the application currency and versioning.

Contractor shall also assist the County with developing, maintaining, and enhancing its application DR process and related documentation.

7.2.8. Application Training

7.2.8.1. Process and Procedures

Application training is defined as the implementation of training programs for contractor personnel to help preserve and enhance their knowledge and understanding of applications.

Contractor shall develop training for new and existing staff on the applications as necessary for M&O activities. When Contractor builds a patch or service restoration release, Contractor shall update the application training plan as needed.

During application operations, Contractor shall provide technical training and knowledge transfer to existing County support personnel, as well as materials related to the technical aspects of applications, as necessary. Contractor shall develop, document, and maintain the Policies and Procedures Manual, training, and knowledge transfer procedures that meet the County's requirements and policies.

In addition to training users, Contractor shall conduct new and refresher training programs for Contractor's personnel to preserve and enhance the knowledge and understanding of the applications and the underlying technologies and frameworks on which they are built. The training shall include industry standard certification as well as external training on the latest releases of databases, middleware, enterprise platforms, and applications as required.

Contractor shall train Contractor's development and M&O staff to support application development and changes when implemented into production. Contractor shall follow ITIL-aligned processes for training documentation. Additionally, Contractor shall develop and conduct cross-training to facilitate smooth transitions between Contractor personnel as required and to make sure backup personnel are in place for each application.

Delivery of End User training, including the location and method of training, frequency of training, and documentation provided with training.

End-User training shall include online training or videos to specialized in-person classes or seminars.

Contractor shall develop online training appropriate to the projects. This may include Adobe Captivate vignettes, videos, or posted documentation and frequently asked questions (FAQs).

For specialized in-person training, the County currently uses the 200-square-foot Contractor/County training center in Contractor's Rancho Bernardo location. Contractor shall continue to maintain and make that space available to the County. The center provides 36 County-imaged desktops hosted on the County of San Diego Network and provides a quiet, controlled environment. The center's simulation environment shall accommodate User Acceptance Testing (UAT) if requested, which allows the County to test features and functionality prior to deployment.

The facility shall provide printing and projection capabilities to support a successful training experience. This facility shall continue to be available as well for County trainers to train County staff.

Major releases may require online and classroom training for the End-User community on a scheduled basis, while minor changes may require only an update to procedures or processes and notification to the End-User to use the new process.

7.2.9. Application Quality Assurance Services

7.2.9.1. Process and Procedures

Application QA services is defined as a systematic, planned set of actions necessary for software update/development processes to conform to established functional technical requirements. It also includes the managerial requirements of keeping the schedule and resources within budgetary confines.

Contractor shall create, update, and maintain a QA management approach for applications updates. This shall include the following QA components:

- Quality management approach
- Effective software engineering technology
- Formal technical reviews applied during the SDLC process
- Multi-tiered application integration and testing strategy and implementation
- Control of software documentation and associate changes
- Procedure to measure compliance with software development standards
- Measurement of QA metrics and reporting mechanisms.

Contractor shall submit Contractor's QA management approach to the County for approval, after which it shall be added and kept current in the Standard and Procedures Manual.

Contractor shall determine QA metrics for each release and reports these to the County. Contractor shall communicate configuration management items, tracking them to Contractor's Systems of Record that accurately depicts the environment. These shall be updated to reflect all new changes, which shall be made with a change record processed through HPE Service Manager that keeps Contractor's information accurate.

7.2.10. Database Administration

7.2.10.1. Process and Procedures

Database administration (DBA) shall be defined as activities associated with the maintenance and support of databases.

Contractor shall define DBA requirements and policies for the application databases, including authorization requirements for end-users, roles, and schemas. Contractor shall develop a Standards and Procedures Manual database administration procedure that meets the County's standards and policies. Contractor shall develop and provide database roadmaps for planning and portfolio management.

Contractor's DBA processes shall document security administration including managing role and End-User database permissions and in accordance with the County security policies. Contractor shall perform database restores when required.

Contractor shall define, document, and execute database creation, configuration, upgrades, patches, refreshes, database system-level changes, schema changes, and definition requirements for applications. Contractor shall maintain documentation for portfolio applications database instance parameters and system settings and manage them across like instances when required during the application change process. Contractor shall provide and execute proactive database performance and tuning scripts and monitor database performance for optimal performance.

Contractor shall implement and manage County-approved appropriate database management tools across application portfolio database instances. Contractor shall capture performance metrics and historical data for trending and reporting. Contractor shall use Oracle Enterprise Manager to manage the Oracle/UNIX enterprise applications. In conjunction with Oracle Enterprise Manager, Contractor shall use the Applications Performance Management (APM) tool to provide a full 360-degree view.

Also, Contractor shall identify and resolve locking conflicts, latch contention, and rollback requirements for database instances and implement database monitoring tools that generate automatic Service Desk trouble tickets for incidents.

Contractor shall provide technical assistance and subject matter expertise to application developers and third-parties. Contractor shall provide data dictionary knowledge, End-User data assistance, data warehouse metadata definition, and data mapping.

Contractor's DBAs shall patch database software as approved and manage database communication software configuration, installation, and maintenance. They also shall provide database storage management and cleanup activities, backup schedules, retention periods and levels, and execute backups and recoveries that adhere to the County's policies.

Contractor's DBAs shall provide database capacity management and availability management, maintain database storage allocation, file systems current usage, and capacity. Contractor shall conduct database installation, de-installation and administration, testing, copying, and security and database server management, as needed and provide administrative account support that shall include provisioning and de-provisioning. Contractor shall create and provide system monitoring and documentation, maintain transactional logs, and backup as scheduled. Finally, Contractor shall provide operational support for the County's public and private cloud databases.

7.3. Application Development Services

- Deployment plan for resources and use of facilities

Staff shall be located at the Contractor's Rancho Bernardo site, El Paso, TX and Pontiac, MI.

7.3.1.1. Process and Procedures

- Applications Development Services

Contractor shall reach out to Third Party providers who can deliver quality apps projects on time and within County budget. Contractor shall work to include applications providers in Contractor's outreach process that currently includes more than 20 different vendors. Contractor shall also reach out to Disabled Veteran Business Enterprises (DVBE) and give them the opportunity to provide services.

Contractor shall continue to work with the County to use COTS and third-party applications where appropriate. On a per project basis, Contractor shall reach out to third-party providers as resources and

expertise is needed. If the County has a requirement for a specific or unique solution, Contractor shall engage with those application providers as described in the "Procurement of Third-Party IT Solution via the ITO" process referenced below.

Contractor shall provide third-party vendors access to the development and test (Dev/Test) environments.

Applications Development Services shall be conducted either on a time & materials basis using Resource Units defined in the Agreement (e.g., labor hours based on the Labor Categories) or on a firm, fixed price basis, at the County's option. A fixed price for Applications Development Services shall be based on defined statements of work, and may include warranty services as negotiated and agreed-upon by the parties.

There shall be two types of estimates for Applications Development Services:

1) Budget Estimate (BE) – A BE shall be generated by Contractor upon County request. The BE shall establish a range, or rough order-of-magnitude estimate based on a statement of work, for County budgeting purposes. Preparation of a BE shall be a non-billable task.

2) Service Request Project Estimate – A Service Request Project Estimate shall be generated by Contractor upon County request. The County shall provide a detailed statement of work and requirements to accompany the request. The County does not anticipate significant overhead to generate estimate, given that the statement of work and requirements are already complete, but solution design, detailed one-time and on-going cost estimates (including the cost and time to bring a development project into the Applications Portfolio), resource breakdowns, and impact analysis shall be billable. Depending on the size of the project, a Service Request Project Estimate may be covered by Service Levels once the project is approved by the County.

When procuring Application Development Services:

1) The County develops a statement of work, either using its own resources or by leveraging Contractor resources using the approved Labor Categories. The result is a specific statement of work to meet the County's business requirements.

2) The County determines the appropriate procurement vehicle, either using the Agreement or pursuing an alternate path (e.g., County Purchasing and Contracting).

3) If the County decides to leverage the Agreement, it may:

    a. **Contractor Estimate:** Issue a Service Request to Contractor either soliciting a time and materials proposal (using the Resource Unit labor rates) or a firm, fixed price proposal. Upon County approval, Contractor shall (a) use its own resources to deliver these services or (b) use its network of Subcontractors to execute the work;

    b. **Request for Information (RFI):** Issue a Service Request to Contractor to conduct a market scan, to be performed by the Acquisition Manager, using the approach set forth in the Standards and Procedures Manual to identify

potential solutions and/or vendors. Contractor shall conduct a market study and provide the results to the County for review. Services performed by Contract and Acquisition Management Services resources shall be covered by the Cross-Functional Services Framework Resource Unit. Assistance by Contractor Applications resources for the purposes of the evaluation shall be billable in accordance with the applicable labor rates upon County approval;

c. **Pre-Approved Vendors Request for Proposal (RFP)**: Submit a Service Request to Contractor and direct Contractor to facilitate a competitive procurement process among a list of pre-approved vendors that have a master agreement with Contractor allowing for rapid execution of Statements of Work ("Pre-Approved Vendors"). Contractor shall provide to County a list of Pre-Approved Vendors as part of Schedule 5.

Contractor shall post County requirements from the Service Request (mechanism to be determined, likely a SharePoint site), alert its Pre-Approved Vendors of the pending opportunity, and require responses within a specific timeframe, which shall be communicated to the County. Pre-Approved Vendors shall be required to respond to Contractor within the stated timeframe with a firm fixed price proposal to complete the Service Request. Contractor shall review the responses and share qualified responses with the County along with a recommendation to proceed (or not). Contractor shall work with the County to select the pre-approved vendor that offers the best value to execute the Service Request based on criteria agreed upon in advance of the competitive process. Upon County approval, Contractor shall contract with the selected pre-approved vendor to execute the Statement of Work (services requested). If this process is used, the Resource Unit labor rates do not necessarily apply for the pre-approved vendor proposal, since the competitive procurement process among Pre-Approved Vendors provides a mechanism for fair and reasonable pricing, assuming multiple offerors. The proposals from the Pre-Approved Vendors shall be submitted to the County at no additional cost to the County; and/or

d. **Request for Proposals (RFP):** Submit a Service Request to Contractor and direct Contractor to facilitate a competitive procurement process among third-party vendors, to be performed by the Acquisition Manager, using the approach set forth in the Standards and Procedures Manual. Contractor shall work with the County to select the vendor that offers the best value to execute the Service Request based on criteria agreed upon in advance of the competitive process. Services performed by Contract and Acquisition Management Services resources shall be covered by the Cross-Functional Services Framework Resource Unit. Assistance by Contractor Applications resources for the purposes of the evaluation shall be billable in accordance with the applicable labor rates upon County approval.

Contractor shall document the foregoing procedures in more detail in the Standards and Procedures Manual.

Pre-Approved Vendors List Management

Contractor shall add Pre-Approved Vendors that (1) are existing vendors that have requested to be Pre-Approved Vendors, (2) have agreed to terms and conditions and (3) have provided proven value to the County. Additional Pre-Approved Vendors shall be added from the larger group of Contractor providers with which Contractor has established master agreements and that provide services applicable to the County. Contractor shall also use all reasonable efforts to add vendors to the Pre-Approved Vendors list in response to County requests requiring frequently used niche skillsets.

Contractor shall maintain no fewer than five (5) Pre-Approved Vendors who are eligible to propose on County applications work. Contractor shall choose vendors based on specialty skills with specific technologies (ex: Captiva, SharePoint) or general skills required by County projects (ex: Project Management).

Contractor shall add Pre-Approved Vendors as identified and compliant; Contractor shall post the current list of Pre-Approved Vendors on the Service Portal

After CY1, Contractor shall add and maintain Pre-Approved Vendors based on County demand as follows:

Number of Service Requests	Minimum Number of Pre-Approved Vendors
< 15	Five (5)
15 - 25	Seven (7)
26 - 50	Ten (10)
51+	Fifteen (15)

At the end of each Contract Year, Contractor shall notify County if Contractor is unable to meet the minimum number of qualifying Pre-Approved Vendors and shall provide County a recommendation on next steps to meet or modify the County's requirements.

- Solution to meet the requirements

Contractor's solution shall use an established Contractor application development framework plan, build, operate to meet deliverables requirements. This framework accommodates Agile, Iterative, and Waterfall methodologies, making sure roles and responsibilities are defined, governance processes are in place, and the work follows a structured approach to achieve its objectives. Contractor's applications team shall tailor the framework.

Contractor's application development framework shall provide a delivery and governance framework covering all aspects of IT-enabled business change. The framework spans the full delivery life cycle, from application development planning through operations. Security shall be managed during the life cycle of the application, from discovery through operations.

Development Process

Contractor's development processes shall follow SDLC, using Agile, Iterative, and Waterfall methodologies as appropriate.

Each project shall:

- Engage key stakeholders
- Identify the business, security and DR, and business continuity and planning requirements
- Analyze the requirements from internal and external perspectives
- Prioritize and select projects that shall be included in the program scope.

For gathering and identifying requirements, Contractor shall leverage the Requirements Determination Process (RDP) that contains five major components: plan/manage, obtain, understand, validate, and evaluate, as delineated in following table. Contractor shall obtain, understand, and validate components make up the core of the RDP. Contractor shall execute these components multiple times, once for each set of requirements.

Five Major Components – Requirements Determination Process

COMPONENT	PURPOSE/ACTIVITIES
Plan/Manage	Contractor builds the plan that Contractor shall follow throughout the process and manage overall execution of the RDP.
Obtain	Contractor collects the information for the business, technical, security and DR, and business continuity planning needs of the County. Contractor shall store the information Contractor obtains for later retrieval and traceability.
Understand	Contractor shall analyze the collected information to make sure Contractor has a good understanding of the requirements. Contractor then evaluates the statements for consistency, completeness, and appropriateness. For each statement, Contractor shall establish traceability and validation criteria and perform RCA.
Validate	Contractor shall confirm a mutual understanding of the implications of the requirements with the County and Contractor SMEs, who shall build and implement the solution.
Evaluate	Contractor assesses how well the process worked and determine the effectiveness of the techniques and the requirements statement. Contractor shall work with the County to prioritize the requirements and establish a roadmap.

During design, project details shall be defined to align with the County's strategic direction.

Requirements are captured and more detailed views of the "As Is" and "To Be" states shall be developed.

For existing applications, Contractor shall review the current state of the architecture and identify the impact of the solution as well as alternative solutions. Contractor shall notify the County of any changes that impacts the current architecture so a decision on solution options can be made early in the development cycle. Contractor shall also conduct industry research to identify any COTS product solutions that may meet the requirements.

The application architecture and its impact shall be reviewed with the County to provide a better understanding of the changes and a solution design document shall be created to document the solution with changes to the application, database and the infrastructure as needed. All design features as well as changes to data models and configurations shall be documented. Detailed procedures to migrate data to the new data models shall be defined.

Once requirements are defined, Contractor shall expeditiously notify external applications providers and invite them to provide a bid for the work.

After selection of an applications provider (Contractor or a third-party), the provider shall develop a detailed project along with an applications roadmap. The following describes various phases and deliverables of the project.

Deliverables for the assets and align phase include:

- High-level application solution design
- Application architecture
- Future roadmap
- High-level project plan.

When the project is implemented, the handover to M&O is executed to include documentation, training, and updated Service Desk scripts.

The project plan shall include details of the application development, testing, integration, and implementation schedules. Contractor shall use Contractor's risk management processes to mitigate risks early in the process. Contractor shall provide detailed project and cost information to the County, and all changes to the plan and cost Contractor shall follow the change management processes established by the County.

Deliverables for the design phase include:

- Detailed design document
- Update architecture document
- Detailed project plan
- Risk and mitigation strategies
- Detailed project cost estimates
- Updated requirements document.

The develop phase shall produce the application code according to the application design. The primary deliverables are application code and test scripts and, when needed, a pilot run of the application. Key activities include:

- Application code development and test
- Gain authorization from the County to proceed to implementation.

During this phase, the needed Dev/Test environments shall be created. As new applications that are targeted to run in the MPC are developed, the Contractor team shall request MPC resources through the provisioning interface, including servers, software, storage, and backup requirements. Once the demand request is received by the system, and the automated parts of the provisioning process complete, the Applications team shall then be responsible for installing, configuring, and testing each application component.

Conversely, as applications are retired or their Dev/Test components are no longer needed for live use, and therefore the associated MPC resources are no longer needed, the Applications team shall submit a service request to de-install the MPC infrastructure for that application. The team shall decommission all of the application components and infrastructure resources for the application environment being retired,

and shall release any licenses through Asset and Configuration Management. If the environment is a Dev/Test environment, the request shall specify whether the environment shall be permanently decommissioned or put into cold storage. If the latter applies, the image shall be preserved on the SAN storage and held in an online inventory, but its compute resources released. Otherwise, all resources shall be released.

Contractor shall not use the MPC for production use, unless an exception is authorized by the County Technology Office. From a Resource Unit (RU)/billing perspective, only moves into and out of MPC for production application environments trigger activity: new RUs are added to billing at the point a production environment is made available for County use. RUs are removed from billing at the point when a request to decommission a production environment is issued and approved (the billing change shall not wait for the decommission process to complete). If a production application moves from a traditionally hosted environment to, the old RUs are removed, and new ones take effect at the point when the MPC environment becomes available for County use. The County shall not be billed for both sets of resource units. The same approach shall apply in reverse if an environment moves from MPC to a traditional environment.

Additions and removals of Dev/Test environments into and out of MPC may trigger a slightly different RU action. Additions of new applications to MPC "draw down" on the pool of available resources. If the application is very large, such that its requirements exceed the capacity available (this scenario shall be the exception rather than the rule), Contractor may need to acquire more resources to expand the cloud. In most cases, the resources shall be available, and the environments shall be added with no change to RU billing. By the same token, removal of applications from the Dev/Test pool shall not trigger a change to RU billing. Moves of existing Dev/Test environments into and out of MPC shall have no billing impact.

During this phase, application developers shall implement the application according to the functional specification and application architecture. The developer shall follow Software Development Lifecycle Standard County process and standards to code, build, and deploy. The configuration changes shall be documented and shall become part of the deployment package. The technical lead shall coordinate integration testing with the developer in the development test environments. The designated testing team shall also perform QA testing and End-User acceptance testing (UAT) and partner integration during this phase.

During the development phase, additional risks may be identified. Contractor's Project Manager shall use the Risk management processes to mitigate these risks. Changes to the project plan and cost shall follow the defined change management processes.

Contractor's project manager shall coordinate with the County to obtain approval for UAT and deployment to the production environment.

Deliverables for the develop phase shall include:

- Application code
- Test scripts, including test plans for the independent test team
- UAT results
- Risk and mitigation strategies.

Implement

After gaining the approval from the County using the successful UAT results, Contractor's deployment team shall prepare the release package for deployment to production. A deployment plan shall be created in coordination with the application users, the integration touch points and the M&O team. The

deployment instructions including the configuration details and the data migration steps shall be outlined and validated before deploying the application.

Deliverables shall include:

- Deployment Plan
- Deployment Package
- Third-party cross-training of Contractor staff to perform required M&O activities, as required.

Manage

Once the application has been deployed in production, Contractor shall provide production support under the Applications M&O Services framework. The project team shall load all documentation, such as the architecture and design documents and the deployment package instructions, to the DocVault site for the M&O team to review. An initial hand-off session shall be provided to the M&O team so that the developers become aware of the changes.

The project team shall coordinate and work with Contractor resources to perform market research and technical trends, and provide new products and services and third-party solutions that may be applicable to the County. The team shall work with the County to evaluate these services and make recommendations. The team's reach-back into Contractor's quality management office shall facilitate the process to provide recommendations on changes to SDLC, leveraging ITIL practitioners and their relationships with Software Engineering Institute (SEI).

High Level Requirements

Alignment with IT strategic plan and roadmaps: Contractor understands the County's strategic plan and transformation roadmap and shall ensure that all technology, innovation, reengineering, and business processes align. The development process shall follow standards and guidelines published by the County's IT governance bodies and the architectures shall comply with County-approved enterprise architecture(s), as well as abide by County security policies and models for system architecture and technology.

Contractor's approach shall begin with analyzing requirements and constraints. Analysis of functional inputs shall inform the business architecture view, which describes the high-level functional composition of the system and shows various actors, usage scenarios, and interdependencies among functional modules. After the first phase of high-level design is complete, the architecture artifacts shall be submitted to County staff, as required, for review and approval. The outcomes of the review shall be addressed by further aligning the architecture with the County's business and technology direction and resubmitted for approval.

Contractor shall recommend updates and revisions to architecture and/or configuration change designs in response to changing requirements, emerging technology, and other activities such as vulnerability assessments and performance analysis. Contractor shall monitor industry trends and best practices and make recommendations to the County for other inclusions in the technology roadmap.

The software development process shall follow the established SDLC process and generate documentation as required by the size and complexity of the project. As required, Contractor shall produce architectural design documents in compliance with the County's requirements and alignment with the County IT strategic plan and applications roadmaps.

Integration with existing data and Applications.

Contractor architects, engineers, developers, and operations support teams shall work in concert to facilitate new components introduced into the environment that are able to function as designed without negatively impacting existing systems or County users.

IT standards, guiding principles, architecture bricks and patterns. Contractor follows all applicable standards and compliance requirements of the County and shall maintain and support applicable CMMI, ITIL, and ITSM standards and industry best practices for the delivery of IT services.

Using Contractor's application development framework, Contractor or a third-party shall design the solutions for the requirements. Contractor shall follow County's IT standards, guiding principles, and architecture bricks. Any deviations shall be identified early in the development cycle.

Planning and Standard Setting: For planning purposes, the Contractor Program Office shall provide budgetary estimates as required and follow standard change control procedures.

Contractor shall follow applications standards and work with the County to refine, improve, and modify as required. Contractor shall use Contractor's Program Quality Office to validate best practices, tools efficiency, and process improvements.

System Documentation. Contractor shall maintain the documents for the County program, with a sustained effort to improve timeliness and accuracy.

Cross-Framework Integration. All of the dependent applications, which are part of the impacted framework(s), shall be identified as stakeholders for developing the new requirement.

Contractor staff shall collaborate with the other framework teams to develop an interface control document, which shall become the guide to perform the integration between the frameworks.

Contractor's independent testing team shall perform integration testing and, where possible, use service virtualization tools to test interfaces.

ITIL/CMMI Practices. Contractor shall operate the County environment using ITIL and CMMI best practices. The Contractor ITSM community provides knowledge, best practices, and lessons learned to everyone supporting the County. Contractor shall leverage these unparalleled qualifications when bringing ITIL and CMMI-based processes to the County and recommend any changes to existing policies and procedures.

Standards

Contractor shall follow County's IT standards, guiding principles, and architecture bricks. Any deviations shall be identified early in the development cycle and communicated to the County. Contractor shall follow existing applications standards and work with the County to refine, improve, and modify as required.

Transition. Contractor's deployment plan shall include a strategy to migrate the application into M&O services. Upon implementing the project in production, Contractor's development team shall complete transition to the M&O team in an orderly, controlled manner that includes reviewing processes and outcomes, capturing lessons learned, and creating formal closure documentation.

- Processes in solution including year-to-year continuous improvement

Contractor shall leverage Agile, Iterative, and Waterfall methodologies as needed for each project. The methodology selection shall be discussed with the County and the necessary process shall be executed based on the needs of each project.

As members of the PMI and ITIL communities, Contractor shall provide training for resources, including acceleration programs for the PMP, CAPM, SPI, ITIL, and other disciplines. Contractor participates in global, regional, and Community of Practice (CoP) groups, including the USPS PPM Community, State/ Local Government/Education (SLED) Community of Practice, and the USPS Business Analyst Community of Practice. In addition, Contractor shall monitor industry standards for emerging methodologies and discuss Contractor's findings with the County.

Processes, procedures and use of tools in new systems planning, SDLC, project management, testing (including methods to engage the County) implementation (including methods to engage the County), post-implementation evaluation/review and transition (including transition support for newly implemented applications). Processes followed by Contractor organization that shall minimize disruption to business operations.

Software Development Lifecycle Methodology and Processes

Contractor shall perform full software development lifecycle (SDLC) process activities for developing and implementing new systems and major scope enhancements to existing and evolving systems.

Contractor shall comply with its governance and enterprise architecture principles as well as its procedures.

For each development project, Contractor shall work with the County's project sponsor to create a project plan. The plan shall detail the customized development approach to deliver the desired results with the best quality in the shortest time. Contractor shall provide a proven development model that are widely practiced in the industry and that Contractor has used previously at the County and on other successful projects.

The following table list software development models along with the general characteristics of each and the type of projects for which each model Contractor shall provide:

Application Development Models

DEVELOPMENT MODEL	CHARACTERISTICS	SUITABLE FOR PROJECTS WHEN –
Agile	• Software is developed and tested in short iterations (1 to 4 weeks) • Adaptive • Iterations are usually time-boxed to limit risk • Software is the principal measure of progress, with less emphasis on intermediate artifacts • Face-to-face communication is preferred to documentation	• Requirements are not well known but can be evolved through short cycles • The project team is relatively small so that developers and customers can easily communicate and incorporate feedback into the next interaction
Waterfall	• Sequential process that flows through requirements capture, analysis, design, coding • Plan driven • Predictive • Low risk • Expected results clearly defined up front	• Requirements are well defined up front and changes are expected to be minimal • System reliability is critical • Documentation requirements are high

DEVELOPMENT MODEL	CHARACTERISTICS	SUITABLE FOR PROJECTS WHEN –
	• Generally, artifact intensive (models, plans, documentation)	• Project team is large and incorporates many disparate organizations

Contractor's applications team adheres to County procedures that can be applied to Waterfall, Agile, or, alternatively, Agile/Scrum.

Contractor shall use the following activities that are common to nearly all projects:

- Business Modeling
- Requirements
- Analysis and Design
- Implementation
- Testing
- Deployment
- Configuration and Change Management
- Project Management
- Environment

Project Management

Overall governance of development projects shall be managed by Project Management. Contractor's ITIL-aligned project management methodology supports recognized industry standards, including the CMMI Institute's Capability Maturity Model Integration (CMMI), Projects IN Controlled Environments (PRINCE2), and the Project Management Institute's Project Management Body of Knowledge (PMI PMBoK) Guide.

Contractor shall use a proven set of tools (like HPE's Project and Portfolio Management Center (PPMC)) to plan, budget, and track cost, scope, and schedule performance data. Contractor shall engage the County in each step of the system development process—from evaluation to deployment.

Contractor shall provide a Service Portal that include access to the County on Contractor service level performance, project schedules, and cost.

Testing

Contractor shall leverage the Contractor's Enterprise Testing (ET) Methodology to plan, develop, and conduct an integrated Test Program. The methodology shall provide County visibility, traceability, and accountability in requirements management and verification; it shall also provide risk identification, management, and timely resolution in support of the County development and maintenance activities, as shown in

Using Contractor's ET Methodology—a comprehensive framework that provides the structure, processes, tools, and templates—Contractor shall align to the County SDLC.

Contractor's test team shall conduct the Test and Evaluation (T&E) program, including managing the creation of test plans and procedures, testing, and developing test reports; communicate the result of testing and recommendations to the team and to the client; and provide input to Contractor's Program Manager on cost, schedule, and staffing for meeting requirements in this area.

Contractor shall prioritize high-risk, high-value business requirements and concentrate testing activity on those requirements to minimize risk and deliver the most value to the County for the application implementation. Contractor shall set the testing strategy based on the value of a business function as well as the potential for failure and the associated risk. The testing strategy applies the highest levels of test coverage to the highest-risk, high-value functions.

Contractor's risk-based, requirements-driven testing has the following components, shall be executed iteratively:

- **Ambiguity Analysis –** Contractor shall conduct an ambiguity analysis to make sure that the requirements document is deterministic (with randomness removed), unambiguous, correct, complete, and testable. Contractor shall systematically analyze ambiguities in the requirements that drive application design, development, and testing to minimize inconsistencies and maximize requirements clarity.
- **Risk Analysis –** Contractor shall systematically analyze risks in those requirements to reduce chances of misdirected or incomplete test coverage, with focus on isolating and mitigating the most critical risks first—those that most negatively affect the highest-priority aspects of an application or system.
- **Systematic Test Design –** Contractor shall use methodical activities focused on managing and mitigating risks, Contractor shall apply test design techniques to plan, choose, and develop the most effective tests to verify from the bottom up to integrated functional areas and interfaces within the complete system for operational configurations and environments.
- **Requirements Traceability –** Contractor shall provide throughout test development and execution, Contractor use a Requirements Traceability Matrix (RTM) to comprehensively depict test coverage and keep testing focused on high-risk, high-priority requirements.
- **Testing Metrics Collection/Reporting –** Contractor testing reports offer ongoing insight into testing progress, coverage, and defect resolution; they offer timely opportunities for acting to mitigate risk before it causes irreversible harm.
- **Testing Close-Down Activities –** While testing ends with all tests executed, all defects resolved, and a system unquestionably ready for release, defects can outlast time and budget limits. Contractor shall focus on satisfying high-risk, high-priority requirements first through risk-based testing, leaving as the last priority tests and defects for only low-risk, low-priority requirements, as agreed upon in the Test Plan.

Contractor's applications group shall use the following tools from Contractor's Application Lifecycle Management (ALM) tool suite: the HPE Quality Center tool for test management and tracking, HPE Unified Functional Test for automated testing, and HPE Performance Center for performance testing. Contractor shall use these tools to manage and develop a series of test scenarios and test cases that test the entire solution for functional and performance quality. Based on the broad scope of Contractor's testing and tools, Contractor shall use automated and manual test scenarios and cases to fully test the solution. Contractor shall manage the test scenarios and cases with the HPE suite of testing products and then link and trace them to the approved requirements.

Implementation

After Test, Installation, and Validation phases have been successfully completed, the implementation process continues with a final review of success factors, associated risks, and mitigation strategy. All of the primary technical functions shall be documented and targeted, making certain that the applications development team and the County business owner agree with the decision to go to production. As documented in the pre-application cutover phase, each functional area shall be reviewed for completeness, functionality, and readiness.

Contractor shall mitigate risks to integration of systems by applying Contractor's consistent, repeatable system integration and project methodology that provide effective communication, coordination, and collaboration with the County, that shall result in a fully integrated solution.

Contractor shall develop a back out plan for each implementation to provide for rapid rollback to the original state if required. Whenever possible, the source system remains up and running until Contractor is sure that the workload has migrated successfully. This approach provides a fully redundant contingency; immediately after implementation, Contractor's Applications Development team shall test the functionality in the production environment to make sure County users shall not experience any disruption.

Transition to Application M&O Services

Upon successful implementation, the Contractor's application M&O staff shall provide support for the production application. Prior to production cutover, the Applications M&O team shall receive cross-training and documentation to provide a smooth transition from the development team. The development staff shall also review with the M&O staff any changes to the design and deployment document as well as the test results.

Application demand management methodology

Contractor's ITIL-aligned demand management methodology uses frequent communication with the County Technology Office to maintain alignment with the County's strategic priorities and schedules for new or modified application deployment.

Demand Management shall be approached with two methods; PPMC Demand Management module and Demand Growth & Innovation

Demand Growth & Innovated Solutions

The Business Analysts (BA)/Solution Architecture (SA) Service Center shall work with the department to ensure their demands are being managed. BAs shall assist the County in identifying and prioritizing future demand. Embedded with County departments, BAs shall work closely with the County users and have a solid understanding and the ability to articulate the departments business needs. BAs shall detect prospects for driving business innovation, aligning IT initiatives with business goals, to the SA and CTA. In turn, the SA/CTA shall work with the CTO to determine which technologies may be required to meet the business need. From that determination, the applications team shall forecast demand by department, technology, and timeframe.

Contractor shall host road mapping sessions including white board activities to better understand business demands, integrate with Contractor's innovation process and provide technology showcases on a regular basis as determined by the County and Contractor. The objective is to define a multi-year roadmap (over 5 fiscal years) to improve departments' ability to plan for change and influence IT direction in the overall County IT environment. The BA/SA partnership is key for defining their architectural/business road maps. The roadmap shall consider four key components:

- High level County/business objectives
- Technology/Vendor Lifecycle Roadmaps (e.g. Windows/Oracle, SQL)
- KPIs to measure roadmap progress
- Department PAIDs and projects

Contractor shall hold these sessions every 6 months or as otherwise determined by the County and shall review road maps, historical trends and map out business group's strategic plans and adjust road maps to meet the technology and business demands.

Contractor demand management practice shall facilitate staff planning, working with the County to identify slowdowns, provide a predictable forecast for budgeting and keep the business move in the right direction.

Demand Management with PPM

The Contractor's application demand management tool shall be HPE's PPMC Demand Management module. HPE PPMC consolidates, prioritizes, and fulfills the strategic application projects activities so the County can redirect activity based on demands.

The PPMC tool lets Contractor consolidate and prioritize the applications requests and focus on the highest-priority County initiatives.

Because the PPMC Demand Management module captures all IT requests, it enables County stakeholders to have a comprehensive picture of past, present, and future IT demands, grouped by demand category.

The PPMC Demand Management module processes a request based on the best-practice process and business rules for that type of request, after each request is captured. The process behind each request is modeled, automated, enforced, and measured. Automated, out-of-the-box, best-practice processes—including proposed projects, application-related enhancements, project scope change requests, non-project related requests, and others—are easily configured to support the County's specific best practices, using a drag-and-drop process modeler.

The module helps responding to new demands and changing priorities by redeploying resources and provides the automated processes and data necessary to effectively manage status, service levels, and trends. Web-based dashboards provide real-time visibility into request status, priority, next steps, and summary views. Service levels shall be updated automatically as each request is processed.

Business rules define when to send notifications so the PPM module can monitor processes in real time and alert the County and Contractor's applications team when something needs attention.

When priorities change, cycle times may be exceeded, or other requirements possibly may not be met, PPM can trigger an escalation process. With this level of visibility and control, Contractor can focus on the highest-priority requests and know quickly whether a project may be in jeopardy.

How HPE PPM Demand Management Works

Each request type shall have an associated workflow, which specifies the process for reviewing, evaluating, prioritizing, scheduling, and approving the request. Based on the workflow, the Contractor reviewer shall assign the request to a person or team for scheduling and delivery. Notifications defined as part of the process shall be activated at any step to indicate work that needs to be done, has not been done, or is being escalated.

With online access, Contractor managers shall assign tasks, and developers can view and work on tasks assigned. Service levels are updated in real time, and changes are captured for a complete audit trail. Contractor shall link the module to the new Service Portal described.

Contractor shall provide the following key features and benefits of PPM Demand Management:

- **Shared demand repository**

- **Unlimited demand categories**
- **Demand scheduling and prioritization**
- **Drag-and-drop process modeling**
- **Complete audit trail**

Contractor's approach for performing system analysis and design for major new development projects and enhancements. Describe how Contractor expects the County to be involved in the analysis and design process.

Contractor shall work collaboratively with the County during the planning, analysis, and design phases of development projects. Contractor shall include the following activities that Contractor shall perform iteratively throughout the delivery life cycle. Contractor shall adhere to the County Standards and Procedures applicable to all applications development projects.

Collaborative Planning with the County – Analysis and Design

Upon receipt of an approved request, Contractor shall kick off the project by conducting a series of workshops with the County project sponsor. Contractor's team's focus during the planning workshops is to facilitate collaborative dialogue with the County on design of the new system. Contractor's expectation is that the County product owner shall describe the intended result so Contractor's team can understand the requirements, begin to design the architecture, and apply technical standards.

During these workshops, Contractor shall discuss "End-User stories" that encourage the County to visualize the new system as deployed. Analysis of the new system shall include realistic assessment of anticipated improvements, potential limitations, and possible risks. Contractor also shall discuss system business rules needed to facilitate continuity from the existing process to the new system. **Error! Reference source not found.**Contractor shall build a roadmap and next steps with the County that sets realistic target dates for solution design, development, testing, and deployment. The roadmap shall define the County's role throughout the development process.

Contractor's approach allows the County to continue to provide design input throughout Contractor's iterative processes, keeping the new system development aligned to County objectives.

Contractor shall maintain SDLC documentation as the project progresses. This shall include documentation of the County's priorities, the solution design and its characteristics and features, results of the collaborative analysis including risk assessment, and the improvements anticipated upon deployment and all approved changes. Based on the planning workshop discussions, Contractor's team shall refine and document the functional and nonfunctional technical requirements and submit them for County approval.

Cloud and E-commerce solutions. Contractor experience implementing E-commerce and cloud solutions.

Cloud Services

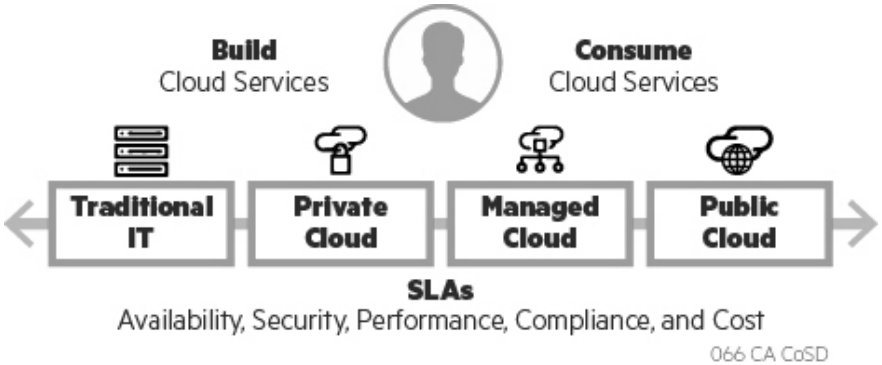
With the planned consolidation to the Tulsa data center, Contractor shall take this opportunity to move the current Dev/Test application infrastructure from a well-performing traditional hosted environment to a more agile, hybrid Managed Private Cloud (MPC) for compatible platforms, and retain the traditional hosted environment where necessary for applications that are not initially cloud compatible. The MPC environment shall be a highly standardized environment with high redundancy and high availability for both infrastructure and applications to eliminate single points of failure. Moving to MPC provides benefits of streamlined server provisioning, enabling Contractor to provision, scale, and de-provision virtual servers in hours instead of days. This shall also include tools that simplify capacity and performance management, monitoring, patching, and security and regulatory compliance and provides the

foundation for the County to take advantage of additional public cloud services. Contractor shall work with the County to identify production applications that are candidates for the MPC environment.

In partnership with AT&T, Contractor shall provide virtualized services for the County. Contractor's network is designed to provide maximum flexibility, enabling adoption of new applications and cloud services while maintaining the highest security and service levels. Acting as an "enabler to the enterprise," Contractor's network shall enable any device managed or unmanaged to be evaluated, authenticated, and allowed policy-based access.

Contractor's solution's End-User-friendly portal shall result in quick adoption, and provide state-of-the-art software for cloud service catalog presentation, automation, management, and orchestration. HPE's Cloud Service Automation (CSA) Portal platform is the End-User entry point into the Cloud Consumer Portal. Users can view service details and subscriptions through an easy-to-use self-service portal.

Full Suite of Cloud and Cloud Broker Services



Contractor's cloud solution shall enable delivery of IT resources as "services"—such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—to consumers using ITIL-based management and operational support processes through a web-based, private Cloud Consumer Portal. Contractor skilled resources shall provide setup, configuration, and ongoing management of the private cloud, so applications development staff can more effectively complete projects.

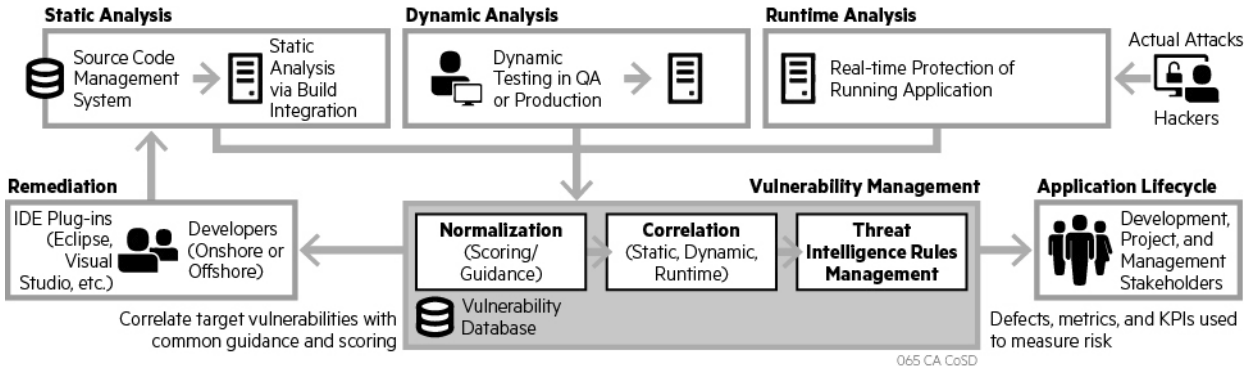
Contractor's CloudSystem shall enable Contractor's development team to build and manage services across private cloud environments on a simplified, integrated architecture:

- Intelligent automation; application-to-infrastructure
- Complete service life cycle management—from provisioning to monitoring to retirement/de-provisioning
- Supports multi-hypervisor, multi-operating system (OS), and heterogeneous infrastructures – now including Kernel-based Virtual Machine (KVM) and Hyper-V support
- Pre-packaged service design tools – HPE Cloud Maps, which are pre-configured and standardized workflow templates for infrastructure deployment, application deployment, and life cycle management;
- Out-of-the-box bursting capabilities broker service delivery across multiple clouds from a single, integrated point of control
- Built on proven and market-leading HPE Converged Infrastructure and HPE Cloud Service Automation (CSA). Combined with Operations Orchestration (OO) and Matrix Operating Environment, CSA automatically enables the design and provisioning of virtual infrastructure services in hours instead of days. Contractor Server Automation software enables Contractor to automatically perform activities such as server discovery to provisioning, patching, configuration management, and script execution to comply with Contractor IT configuration standards.

Security

Contractor's cloud solution shall provide capability to perform Static Code Analyzer (SCA). This service focuses on implementation of the Static Analytics, Remediation, and Vulnerability Management of the architecture in the following figure.

Essential Building Blocks of a Mature, Secure SDLC for Cloud Services



Contractor shall provide a, short-track implementation into the County environment that shall result in a scan of the target application. This shall enable Contractor's team to accomplish the following:

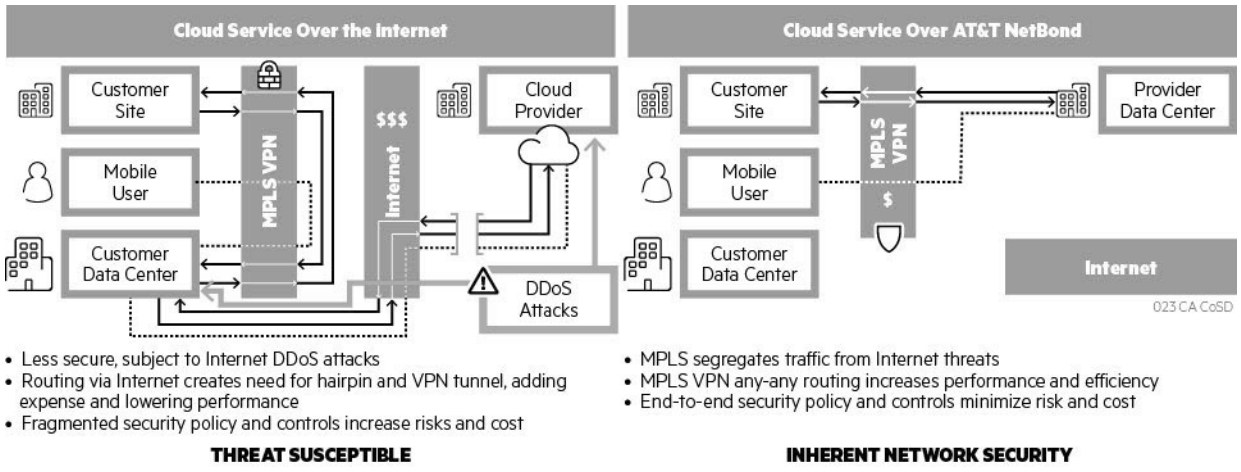
- Produce SCA scans
- Triage scans results to identify and prioritize security vulnerabilities
- Incorporate the Contractor solution for the County into the development process

Embedding Contractor's solution within the software development lifecycle shall enable secure development practices and shall keep applications protected from external threats.

In the background, Contractor's network security is built on AT&T cloud security.

The following figure shows the AT&T NetBond as a basis for cloud services for the County.

Cloud Service over AT&T NetBond



Contractor avoids the security risks of the typical cloud service over the Internet by providing end-to-end security with NetBond.

HPE Cloud Service Automation (CSA) goes beyond traditional IT provisioning; it increases agility and reduces costs. This solution shall offer the following:

- Leverages a modern, easy-to-use self-service portal with an intuitive shopping cart experience for ordering infrastructure and application services across both private and public cloud environments.
- Enables an open, heterogeneous, and extensible architecture supporting OpenStack-based cloud standards, with multi-hypervisor, multi-vendor hardware support that avoids the pain of vendor lock-in.
- Embraces existing automation assets in a highly automated cloud lifecycle management platform that uses an enhanced orchestration engine.
- Designs and orchestrates full-stack services with topology service designs for faster time to value
- Stages complex multi-tier applications with sequential service designs
- Gains enterprise-grade service management with a highly available architecture, providing informed, transparent IT service delivery for secure and compliant services.
- Creates an IT service control point, enabling hybrid IT management across the expansive HPE Helion portfolio of private, public, and hybrid cloud services.

The solution features an open, extensible architecture that supports HPE and third-party management tools, enabling Contractor to quickly adapt to changing business requirements while supporting heterogeneous IT environments.

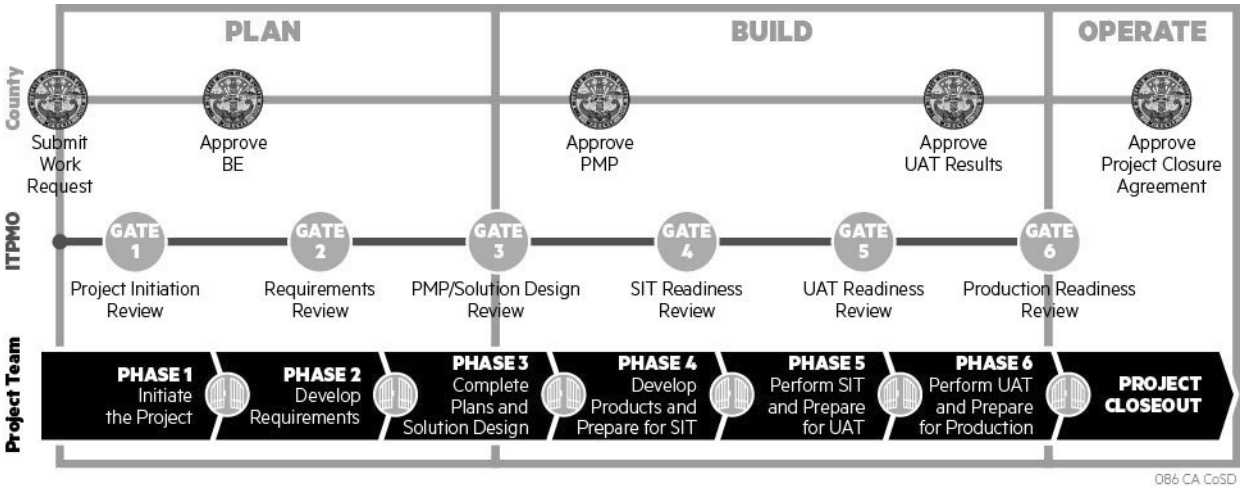
Waterfall and agile development

Contractor shall use Waterfall or Agile approaches based on best fit for the project.

Waterfall Approach

In Waterfall life cycles, each phase (Define and Analyze, Design, Build, Test, Release, and Deploy) is typically executed sequentially, possibly with overlap but with little or no iteration. Contractor shall use Waterfall life cycle development for projects that require a Waterfall approach to deliver business applications or to implement major application enhancements for an existing system.

The County's Waterfall Methodology and Gate Review Approach



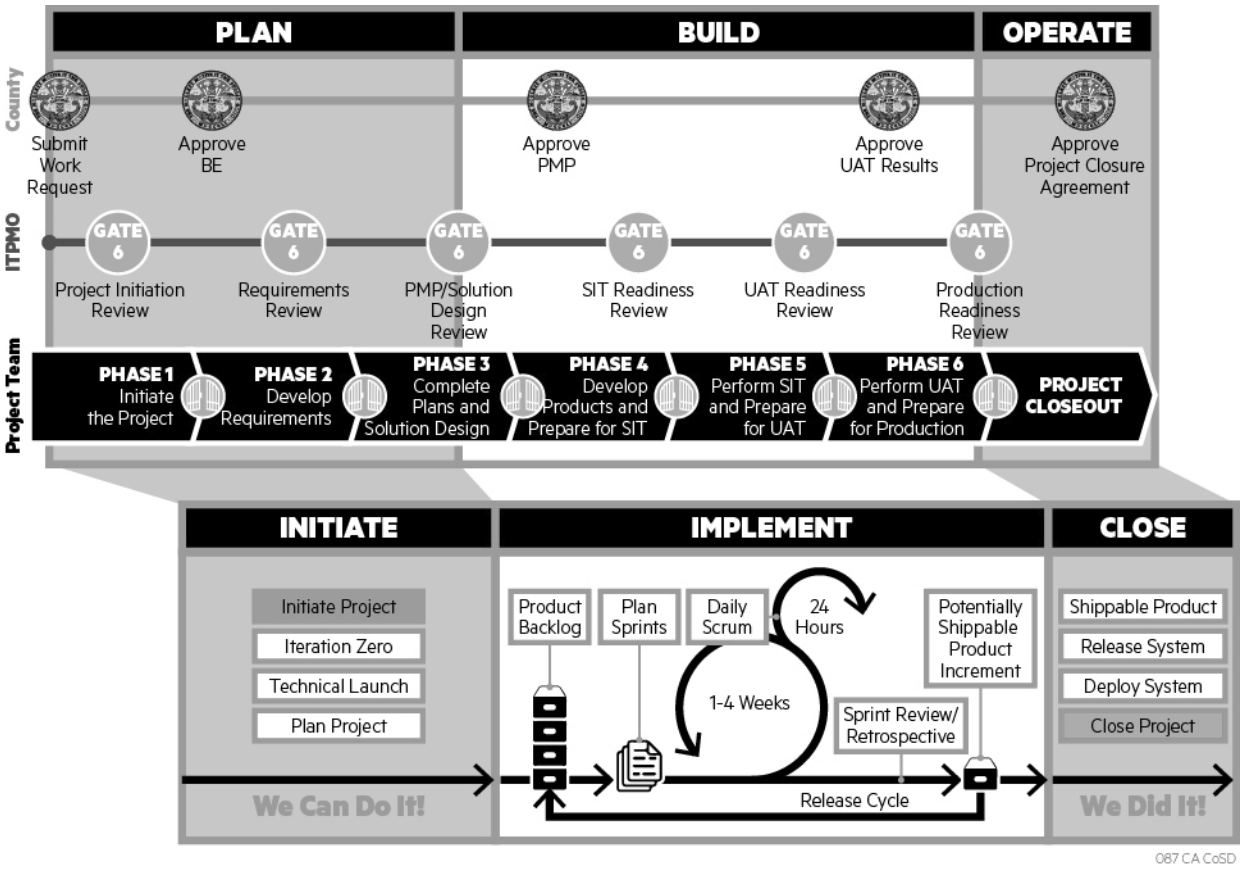
Agile Approach

Contractor tailors an Agile development approach for each project. Based on the Scrum framework, this approach uses an appropriate selection of sound engineering practices from Extreme Programming (XP). It provides a substantial benefit by enabling rapid scalability if required, taking advantage of teams working concurrently in multiple locations, while preserving the ability of rapid response to change.

Scrum Framework

Contractor shall use Scrum Framework process for projects that require a Scrum approach to deliver business applications or to implement major application enhancements for an existing system.

Using County Waterfall Gate Reviews with Contractor Agile Development Process



Contractor maintains County procedures during Contractor's Agile/Scrum development.

- Automated Tools – Automated systems and tools involved in solution

Contractor shall use tools such as HPE's ALM and Dell Marketing's Toad for Oracle software. Contractor shall evaluate other tools that can be used to automate application development services activities and make appropriate recommendations. Contractor shall evaluate automation in configuration and release management as well as the use of HPE cloud service automation and HPE Codar to bring in automation for release management and to integrate with server builds to implement DevOps capabilities.

Contractor's applications development team shall use Contractor Project and Portfolio Management (HPE PPM) demand management module to centralize the resource assignment process. This allows Contractor to strategically manage Contractor's workforce to meet the County's demand across the enterprise. Contractor shall use PPM to track actual effort against project work, allowing quick access to level of effort information that shall be used to inform decisions and prioritize work across all county projects. PPM also has a powerful workflow process engine that helps automate business processes.

8. TRANSITION SERVICES

8.1 Transition Services

Schedule 2.1

Executive Overview

Contractor shall use Contractor's transition and transformation methodology (TTM) as the basis for managing the overall transition as well as the transition projects. TTM shall provide a comprehensive yet flexible, ITIL-aligned framework so that every aspect of the transition is accounted for, planned for, and expertly managed. The Transition Services Management Office (TSMO) shall have primary responsibility for planning and executing the Transition Plan. Contractor shall define and identify key linkage points in the County of San Diego organization. Contractor shall assign a senior and experienced Transition Services Manager (TSM), who shall direct and lead all aspects of the Transition and shall work collaboratively and transparently with the County assigned TSM and Contractor's existing Program Management Office (PMO). The TSM shall facilitate daily stand-up calls and issue weekly status reports to provide transparency and make sure that key decision-makers and the County stakeholders are fully aware of progress as the transition program proceeds.

The TSM shall lead a clearly defined TPMO, with full accountability for execution. The TSM shall report directly to Contractor's Account Executive. In partnership, they shall execute on-going operations and the transition projects.

Requirements

- Description of solution to meet the requirements

Solution Summary

8.1.1 Communications/Governance Plan for the County and the Legacy Provider

Contractor shall provide a Communications and Governance Plan as part of the Transition Initiation activities.

8.1.2 Contingency Planning/Risk Mitigation

Contractor's Transition and Transformation Methodology (TTM) shall include a robust process for Risk Management that shall make sure risks are mitigated to the County's satisfaction.

8.1.3 Measurable Success Criteria

Each project shall, at its inception, include a step where Contractor and the County mutually agree on the definition and measurement of success. This shall provide a smooth cutover process as each framework and project is completed. Success criteria are of two types:

- Project management success criteria:
  - Signoff of tasks and deliverables according to the dates in the project plan. This shall be measured and reported weekly according to task completion.
- Project deliverable success criteria:
  - Verification that the business objectives set out for the project were met.

The Transition Services Manager shall be responsible for defining the overall success criteria for the program and submitting it to the County for approval, which approval shall not be unreasonably withheld.

Upon such approval, each Transition Project Manager shall be responsible for managing to and measuring the success criteria for each project under his/her purview. Measurements and tracking against defined criteria for each project shall be reported to the joint Transition Services Management Office (TSMO) weekly. Any measurements that indicate that one or more success criteria are in jeopardy shall be escalated to Contractor leadership for remediation.

Measurement of success criteria may be discrete (pass/fail: either the criterion was met or it was not) or continuous (measurable on a scale, such as a range of percentages). Since project deliverable success criteria is relevant to the County, following are some examples of project deliverable success criteria suggested for this program, along with their measurement approach. This is not intended to be an exhaustive list: as previously noted, actual success criteria shall be established for each aspect of the Transition.

PROJECT	DEFINITION OF SUCCESS	MEASUREMENT APPROACH
Overall Transition Program	Sustainment or improvement in customer satisfaction	• Service Level Measurement, before, during, and after the Transition • Periodic customer surveys, specific to the Transition experience and effectiveness of communications
Disaster Recovery Plan	Completion of one table-top or actual failure exercise according to the new plan	Record levels of participation, scope, and end results and remediation recommendations
Data Center Consolidation	Sustainment or improvement in application performance	Verification by stakeholders that an application migrated to the consolidated data center environment performs as well as or better than it did in its previous environment (as measured by batch job execution times or transaction response times; measurements shall be taken and compared against established baselines conducted and documented prior to Transition, using existing tools such as Autosys or Load Runner or using system based monitors such as performance manager
Email Migration	95% of mailboxes migrated in the first pass without subsequent issues, post-pilot; all remaining issues resolved within 24 hours.	Project team migration results report
Storage Architecture	Zero data loss	Verification from migration tools of successful completion

PROJECT	DEFINITION OF SUCCESS	MEASUREMENT APPROACH
Development/Test Environment	Successfully implemented Broker and Managed Private Cloud, with all assets assigned to the correct pools	Audit of assets before and after project to verify assignment
Service Portal	80% of End-Users trained on Portal features	Measurement of End-User participation in training

8.2 Transition Project Plan

During Transition Initiation, Contractor shall work with the County to develop the lower-level details of the project plan.

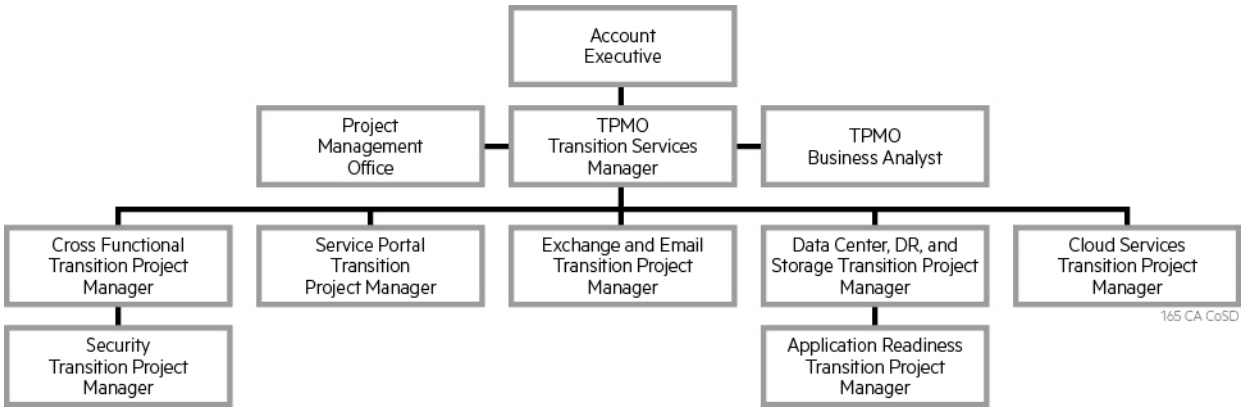
The plan information for each framework can be found as follows:

FRAMEWORK	TRANSITION PLAN
Service Desk	• Cross Functional Transition Schedule and Tasks
Application Services	• Cross Functional Transition Schedule and Tasks Special Cross Functional Projects – Application Services Framework,
End User Services	• Cross Functional Transition Schedule and Tasks
Network Services	• Cross Functional Transition Schedule and Tasks
Data Center Services	• Cross Functional Transition Schedule and Tasks • Special Cross Functional Projects – Data Center Services Framework, • E-Mail Services • Development and Test Environment • Consolidated and Single Data Center • Storage Architecture
Cross Functional Services	• Cross Functional Framework Transition: Activities Aligned to Framework Components • Special Cross Functional Projects

8.3 Transition Staffing

The figure below shows the TSMO structure and the roles, functions, and key responsibilities of each member.

Transition Services Management Office



Dedicated Transition Project Managers shall drive each project's success while managing to the integrated plan.

The TSMO shall create and refine joint program schedules, manage risks, resolve issues, provide proper communication, assess progress, and facilitate on-time transition completion. The TSMO shall serve as a central conduit for information, communication, and cooperation. In addition, the TSMO shall manage all project reporting and quality assurance activities to verify that Contractor follows all established Project Management standards and that project reporting is consistent.

Additional details on roles and responsibilities for the identified TSMO staff are presented in the following table. Each Transition Project Manager shall be responsible for the following items:

- Establishing and documenting progress on their individual sub-project plan(s) within the overall master schedule, and coordinating interdependencies with other projects
- Managing the activities of the technical teams working on their projects, in coordination with the current Contractor support staff and within the established operational delivery processes
- Reporting project status to the TSMO with the Project and Portfolio Management (PPM) tool
- Managing issues and mitigating risks that arise, with escalation when appropriate
- Making sure that their project team meets established success criteria and facilitating handoff of the project's deliverables to operations leadership
- Performing close-down of the program.

The role of each TSMO team member is briefly described in the table below.

TSMO Roles and Responsibilities

TMO ROLES	TRANSITION RESPONSIBILITIES
Transition Services Manager	The Transition Services Manager oversees the Transition results, deliverables, schedules, and dependency tracking across all Transition projects. He is responsible for all Transition activities, including Transition kickoff sessions, program and project management, risk management, communication, reporting, Transition escalations, change management, quality management, operational readiness reviews, and coordination with any in-flight projects. The Transition Services Manager performs quality checks during Transition, working with the Contractor account team to make certain that the team conducts all activities in accordance with established practices.

TMO ROLES	TRANSITION RESPONSIBILITIES
Service Portal Transition Project Manager	Responsible for the project to implement and customize the Service Portal, within the Service Desk Framework.
Data Center Consolidation Project Manager	Responsible for the Data Center Consolidation Transition project within the Data Center Framework. This shall include the following projects: • Buildout and migration to the new Data Center Network compartment in Tulsa, and establishment of connectivity to the disaster recovery (DR) site (Contractor-defined sub-project). • Buildout of the new Storage Architecture. • Establishment of the new DR infrastructure to support subscription services in the Colorado Springs HPE Continuity Center. • Execution of the consolidation of all County Data Center workloads currently residing in Plano into the Tulsa Data Center.
Cloud Services Transition Project Manager	Responsible for setting up and configuring the Managed Private Cloud (MPC) and the Helion Managed Cloud Broker (HMCB) in the Tulsa Data Center and configuring the Development and Test Environment within the Data Center Framework.
Application Readiness Transition Project Manager	Works with the Data Center Consolidation Transition Project Manager to coordinate application migration schedules, plans and testing.
Exchange/Email Transition Project Manager	Responsible for migrating the County to the Office 365 email solution within the Data Center Transition Framework
Cross Functional Project Manager	Responsible for the following projects within the Cross-Functional Framework: • Oversight of the delivery of new Standards and Procedures, Service Level Management and Reporting artifacts (or updating current versions to meet the Agreement requirements) for all Cross-Functional Framework Components, as well as for the other Frameworks • Management of development and implementation of the Cross-Functional Framework Component Management Plans • Coordination of delivery of Disaster Recovery Plans for each Framework.
Security Transition Project Manager	As part of the Cross-Functional Framework, the Security TPM shall be responsible for coordinating execution of Security and Identity Management related projects and changes within the other Frameworks.
TSMO Business Analyst	Responsible for administrative support, such as coordinating status reports and meetings, project schedule change management and integration, and quality management on project deliverables.

Contractor's Transition Management Office shall be staffed and ready to begin as of the Contract Effective Date.

During the Transition period, Contractor shall augment Contractor's technical staff with additional resources to make sure the Transition projects execute successfully, without creating undue constraints on the current support teams. Where appropriate, Contractor may temporarily backfill select members of the

local team supporting the County so that they may lend their expertise and County knowledge to the implementation of some Transition projects. Contractor shall make sure, however, that this does not cause any disruption to the County's current services and projects.

Rationale

Contractor shall manage each sub-project as a project, while continuing to provide excellent service delivery. During the Transition period, Contractor shall successfully plan, communicate, and manage the transition activities collaboratively.

- Deployment plan for resources and use of facilities

Resources. Contractor shall provide dedicated resources for Transition project management and execution to make sure that operational delivery and the County's in-flight projects are not impacted by resource constraints.

Facility. The Contractor Transition teams shall support the Transition from Contractor's Rancho Bernardo site and existing County locations, where appropriate, as well as Contractor's facilities in Tulsa, OK, and Colorado Springs, CO. TSMO resources, including the Transition Services Manager, shall operate out of the Rancho Bernardo site.

- Key methodologies and processes in solution

Contractor shall execute project management, transition, and transformation by using Contractor's Transition and Transformation Methodology (TTM) composed of standardized processes, methods, tools, and governance to deliver repeatable and predictable results. It shall address the people, business processes, and technology issues of transition and provides a step-by-step process for joint planning, communication, post-contract verification, and management.

Contractor TTM Process

Contractor shall use Contractor's comprehensive and proven TTM, a flexible comprehensive framework of robust processes, procedures, best practices and supporting assets that enable the successful planning and execution of a Transition or Transformation program. It shall define what deliverables are to be produced, what work needs to be done, who should do it, how they should do it, and when it needs to be done. It shall also provide supporting assets to complete the work efficiently.

Transition programs and their associated projects shall go through five distinct phases: Initiate, Plan, Execute, Monitor and Control, and Close.

Initiate. Contractor and the County shall set up the program management structure described above, onboard the program team, and start the program. During the first few days of the Transition, Contractor's TSMO shall create draft versions of the Communication Plan, Governance Plan, and the initial master Transition Project Plan and Schedule. Contractor shall start from Contractor's template repository and work with the County collaboratively on these items, but shall also submit a final draft for formal County approval as required. Once finalized and approved, Contractor shall put these plans into action and begin program execution.

Plan. Building on the notional Transition Plan developed during the proposal process, Contractor shall conduct detailed joint planning to elaborate and refine the plan, then conduct a transition kickoff meeting with identified key stakeholders from the County, the current delivery leadership—as represented by Contractor's key personnel—and key leaders from the Transition Technical teams.

The TSMO shall create a master Transition Management Plan along with a corresponding Transition Schedule. This shall serve as the overall foundation for the program and shall address the key program elements, including resources, dependencies, and timeframes. This master plan and schedule shall be augmented for each of the six Transition projects. The figure below provides a high-level timeline of Transition activities, showing the Transition Initiation, the Framework Transitions, and the Final Transition Milestones that follow at the end of the Transition period.

Execute. Within the TTM methodology, each Transition Project Plan shall be executed as described in the sections that follow.

Monitor and Control. Throughout the program, the TSMO shall oversee the Transition activities to produce deliverables on time, remain within budget, and execute Change Management if needed.

Close (Final Transition Milestones). Contractor shall ensure that commitments and success criteria defined in the Transition Management Plan have been met.

- Automated systems and tools involved in solution

The following table lists the tools Contractor shall use to support the Transition program.

Tools Utilized to Support Transition

TOOL NAME AND VENDOR	DESCRIPTION
TTM Templates	• Integrated Transition and Transformation Plan (ITTP) • Transition Specific Risk Register (Excel) • Communication Plan (Word) • Governance Plan (Word) • Transition Daily, Weekly Meeting minutes (Word) • Operational Readiness Checklist / Success Criteria (Word)
Project-specific Tools	• Contractor shall use Microsoft Project to coordinate and manage Transition-related projects and tasks. • Tools used for Transition projects shall be defined and covered in the related sections.

8.3.1. Transition Management Specific Questions

Transitioning licenses, contracts and leases from the Legacy Provider and the County

Contractor shall support and manage all third-party vendor relationships, licenses, contracts, and leases.

Contractor shall create and submit for County approval a process to transfer licenses, contracts, and/or leases, that are included within a Service provided under the Agreement.

Transition resources that shall remain to provide Operational Services for the County versus resources who shall transfer after Transition

Contractor shall provide dedicated resources for each transition project. Contractor shall leverage Contractor resources supporting the County and Contractor's staffing plan shall include subject matter experts (SME) to augment and make sure that there are no impacts to operations activities.

Cross Functional Services

- Description of solution to meet the requirements

Solution Summary

Contractor shall implement Security and Identity Management changes required to meet each framework's delivery model, in those cases where changes are required. The cross functional activities for each framework shall be implemented in parallel but in coordination with that Framework's Transition projects, where applicable. For frameworks that do not have specific transition projects identified, the Cross Functional Transition shall be the only scope of that framework's transition.

During the Transition period, Contractor shall develop a management plan for each of the Cross Functional component areas and train Contractor's teams on the changes. For the Cross Functional components, Contractor shall update the Standards and Procedures Manual, Service Level Management, and Reporting during the 270 days of the Transition period, so these efforts shall follow a similar approach to that of the other frameworks.

- Deployment plan for resources and use of facilities

The Cross Functional Transition activities shall require input and participation from Contractor support staff to make certain that processes and deliverables leverage existing artifacts and methods. The Cross Functional Transition team shall be embedded with each Framework Transition team.

Contractor shall support the Cross Functional Transition primarily from Contractor's Rancho Bernardo site.

- Key methodologies and processes in solution

Transition Schedule and Tasks

The chart below is a high-level example of the Cross Functional activities within a Service Framework: End User Services. The same task structure shall apply to each framework as well as each Cross Functional component.

While the task structure shall be the same across frameworks, task durations shall vary based on the degree of change being introduced by the Agreement requirements.

Although many activities shall happen in parallel, once Contractor creates the schedule for all Cross Functional components and the Cross Functional activities for each framework, the timeline shall expand with the details and dependencies.

The figure below shows the core high-level tasks Contractor shall perform for each framework.

There are no dependencies identified for generation of the Cross Functional Component Management Plans, which shall be developed in parallel with, and as the culmination of, the other component artifacts.

Cross Functional Activities Aligned to Service Frameworks

Within each Service Framework, Contractor shall follow the basic task structure illustrated in the figure below.

Standards and Procedures. Contractor shall inventory and review each procedure document against the Agreement to identify the subset of processes that need to be changed or created (if a new process is needed). Contractor shall then categorize the documents based on the degree of changed required:

- Completely new procedure or standard needed – If a new process is being implemented in support of a new technology, Contractor's Solution Guide documentation for the service offering that Contractor is implementing shall provide a base set of procedure documents. From there, Contractor shall customize and adapt those base documents to the specifics of the County's environment and documentation standards. Contractor shall then test the procedure and further refine the documentation. If a new procedure is needed based on a new business requirement, Contractor can use Contractor's Enabling Delivery and Global Excellence (EDGE) repository to locate a base artifact from which to build the new procedure.
- Updates required to an existing procedure – Contractor shall follow a similar process to the one for a new procedure/standard, but the starting document shall be the existing process. Whether testing is required shall depend on the degree of change.
- Existing procedure continues unchanged – No modifications required.

Once the Standards and Procedures drafts are complete, Contractor shall submit each draft to the County for review and response. The County shall reply within the agreed timeframe if any changes or clarifications are required. Contractor shall then make the final set of modifications, if needed, and finalize the documentation. Documents shall be posted to the appropriate repository reachable from the Service Portal. Any procedures or standards that are no longer valid shall be retired and their documentation archived according to Contractor's Records Management policy.

Where appropriate, Contractor shall provide training in and/or communications about new or modified procedures and standards to Contractor's staff and to County stakeholders who participate in or are customers of the process. Training methods shall range from Frequently Asked Questions (FAQs) and tip sheets, to training videos accessible from the Service Portal, to webcasts or onsite training at Contractor's Rancho Bernardo site.

Service Level Management. During the Cross Functional Transition, Contractor shall adhere to the following steps to implement Service Levels:

For each new or modified Service Level, Contractor shall identify the data necessary to calculate it, the process to verify data quality and scrub exceptions, and any scripting or automation needed to manage the data and its reporting to the Service Level Management process.

Contractor then shall develop and test the new or updated metrics collection process, checking the data and the performance metrics.

Contractor shall identify the appropriate process or service improvements needed to meet the Service Level and test them for an additional month to determine whether this brings Contractor to an acceptable level of performance. Generally, no more than one to three iterations of baseline measurement and adjustment are required to identify the scope of operational change required by the Service Level. The time to complete this process shall be within the time allocated for transition of the applicable framework.

Once Contractor has successfully achieved the new performance target, Contractor shall proceed to update all process and reporting artifacts, and present them for County review and response, according to the steps described above in Standards and Procedures. After finalization, Contractor shall post all deliverables to the appropriate repository, available from the Service Portal.

Once implemented, Contractor's Service Level metrics shall be integrated into the Service Level Dashboard), available from the Service Portal.

Reports/Deliverables. Transition activities for creating new or modified reports shall be similar to the tasks defined for updating Standards and Procedures: Contractor shall inventory and review each report against the Agreement to identify the subset of reports that need to be changed or created. Contractor shall then categorize them based on the degree of changed required:

- New report needed – If a new report is being implemented in support of a new service, Contractor shall create or customize and adapt existing deliverables, or the automated scripts that create them, to the specifics of the County's environment and reporting standards. Contractor shall then test the report and further refine the process. If a new deliverable is needed based on a new business requirement, Contractor can use Contractor's EDGE repository to locate a base artifact from which to design and automate the new report.
- Updates required to an existing report – Contractor shall follow a similar process to the above, but the starting point shall be the existing report process.
- Existing report continues unchanged – No modifications required.

Once drafts of the new or modified reports for the framework are ready, Contractor shall submit them to the County for review and response. The County shall reply within the agreed timeframe if any changes are required. Contractor shall then make the final set of modifications, if needed, and finalize the generation procedures and formats, and place the reports into an automated schedule wherever possible. Process documentation shall be posted to the appropriate repository, as described above, and new reports shall be added to the standard reporting cycle.

Where appropriate, Contractor shall provide training in and/or communications about new or modified procedures and standards to Contractor's staff and to County stakeholders who participate in or are customers of the process. Training methods shall range from FAQs and tip sheets, to training videos accessible from the Service Portal, to webcasts or onsite training in Contractor's Rancho Bernardo site.

Security and Identity Management Updates. In general, transition tasks shall follow the steps illustrated in the Gantt chart, but for security sub-projects, Contractor shall add more detail shall to address specific requirements.

Framework Disaster Recovery Plan. Contractor shall add disaster recovery (DR) specialists to augment the team. They shall be dedicated to maintaining these plans and overseeing DR testing. They shall join the Cross Functional team during transition to lead the DR plan updates for each framework. Each framework shall have its DR plan reviewed and updated to support the requirements of the Agreement. The DR plan shall be submitted in draft form for County review and comment, then finalized and delivered to a restricted area of the Service Portal no later than 90 days prior to the framework cutover[1].

Special Cross Functional Projects – Service Desk Framework

No special Cross Functional projects have been identified for the Service Desk Framework. The project to implement the Service Portal is described in the section for Service Portal transition.

Special Cross Functional Projects – Application Services Framework

Two special Cross Functional projects have been identified for the Application Services Framework that are illustrated in the table below.

Special Service Levels: Application Availability and Application Response Time. The process to implement these two Service Levels shall be similar to that described above.

SaaS Application Onboarding: The County has identified in the solicitation 169 applications identified as SaaS applications that Contractor does not currently support. For each of these that the County wishes Contractor to support, Contractor shall need to perform the steps described in the Gantt chart below.

Contractor shall review each application that the County wants Contractor to support, according to Contractor's established process for Third Party Agreements, and determine the level of support possible for each (license transfer, right to use, warm transfer). Once Contractor has a final list, Contractor shall work with the support contacts at that vendor to understand their support process, and create Service Desk scripts that shall enable Contractor's team to field those calls. Contractor shall then train Contractor's Service Desk staff to support them, and prepare communication materials for users of those applications to understand the new support process.

All draft materials shall be submitted to the County for review and comment. The County shall reply with any changes required within the agreed timeframe, after which Contractor shall finalize and post all deliverables to the Service Portal and cut over support for those applications during the Application Services Transition.

Special Cross Functional Projects – End User Services Framework

No special Cross Functional projects have been identified for the End User Services Framework.

Special Cross Functional Projects – Network Services Framework

No special Cross Functional projects have been identified for the Network Services Framework. The re-architecture and refresh of the Tulsa Data Center network is described in the Data Center Consolidation Project.

Special Cross Functional Projects – Data Center Services Framework

A number of security projects have been identified for the Data Center Services Framework. These include the following:

- Projects to re-orient services that are active-active across sites in the two-data-center model, such as Active Directory, Active Directory Federation Services (ADFS), and the Endpoint Threat Protection core.
- Projects in support of the email transition to cloud, such as adaptation of the Security Incident Management process.
- Projects to address heightened security requirements, such as expansion of security information and event management (SIEM) services, design and implementation of a separate Development/Test network zone, and implementation of continuous scanning.
- As part of the Data Center network buildout, Contractor shall convert from Checkpoint firewalls with TippingPoint for intrusion detection/prevention services to Palo Alto devices that support both functions.

Special Cross Functional Projects – Replacement of myRequests

During the Cross Functional Transition, Contractor shall replace the myRequests Service Request system with the Service Catalog and Request Manager that comes pre-integrated with HPE Service Manager. Because this migration takes longer than the Service Portal implementation, during the initial deployment of the Service Portal, the Service Portal shall be linked (using a front page tile or from the "Links" tile, at

the County's discretion) to the myRequests system, and Contractor shall maintain myRequests following Contractor's processes, while the new request manager/service catalog functionality is being configured. Once the new Request Manager system is ready, and End-User training has taken place, Contractor shall disengage the link to myRequests and bring Request Manager online.

Special Cross Functional Projects – Identity and Access Management (IAM)

Contractor shall provide the following Identity and Access Management implementation services as part of Transition, with ongoing support included in the IAM RU:

- Initial IAM plan for County approval
- Identity Provider capability (Oracle Federation Manager) for the initial use case up (i.e. DCSS) for a maximum of five (5) applications
- Attestation functionality for County review of End-User access. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part and the On-Boarding of the first five (5) applications utilizing provisioning via automated workflow process.
- Capability for County to track and maintain End User access privileges for County users. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part 1 project as well as the implementation of attestation functionality.
- Monthly reporting on changes to the IAM repository. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part 1 project and the onboarding of the first five (5) applications utilizing provisioning via automated workflow process.
- Institute an architecture principle in the design phase of new applications that designates IAM as the single solution for County identities and the use of the enterprise sign on function
- "2.18.2.5 IAM Workflow Automation" project for the amount of $1,633,874.113 consists of two parts as follows:
    - "CSRF Replacement Workflow Automation" – Contractor shall complete the Workflow Automation project and associated requirements for a firm fixed price of $1,228,874. High level descriptions are below:
        - An automated workflow to assign access management requests. The automated workflow process shall create the appropriate line items for the access management teams to manually provision the IDs. Note: this extends past transition since data population is dependent on the completion of Phase I (County funded project) of On-Boarding The Computer Service Requests Form (CSRF) shall be retained for future review and reporting functions as an audit trail.
        - Onboarding up to five (5) applications, at County sole discretion, to utilize provisioning via the automated workflow process, after project completion. Note: this extends past transition since data population is dependent on the automated interface to PeopleSoft part and the On-Boarding. Candidate applications must be only provisioned via Active Directory group membership.
    - "PeopleSoft On-boarding Phase II" – County shall fund and Contractor shall complete the PeopleSoft On-boarding Phase II project for a work effort up to and not to exceed

$405,000. Contractor shall make all reasonable efforts to complete the project within the $405,000 to the best of the Contractor ability. Any work effort exceeding $405,000 shall require a County-approved Change Request to be funded by the County. This project is dependent on the completion of the PeopleSoft On-boarding phase I, which is in progress, and it is County funded under County Work Request SD-WR-024804. PeopleSoft On-boarding Phase I is intended to be completed June 2017.

Cross Functional Framework Transition: Activities Aligned to Framework Components

For the Cross Functional Framework components, the Transition shall follow the same basic structure as described above for the frameworks. The table below summarizes the approximate scope of change in each Cross Functional component. The extent of change to each component has been categorized as follows:

- Limited – changes are expected to be minor updates to existing processes and deliverables
- Medium – some new processes or deliverables—generally similar to current practices
- Large – multiple new processes or deliverables—Organizational Change Management applies

Approximate Scope of Change for each Cross Functional Component

FRAMEWORK COMPONENT	EXTENT OF CHANGE	SPECIAL PROJECTS OR CONSIDERATIONS
Contract and Acquisition Management Services	Minimal	None
Integrated Asset Management Services	Limited	Contractor shall integrate data from AT&T Asset Management Systems
Billing Management Services	Limited	Setup of billing processes for new Resource Units
Security Management Services	Large	Multiple Security sub-projects within the Data Center and Network Frameworks, as described above.
Service Delivery Management Services	Medium	New component
Project Management Services	Limited	None
Integration and Testing Services	Medium	New component
Incident Management Services	Limited	New component
Problem Management Services	Limited	New component
Change Management Services	Limited	New component
Release Management Services	Medium	New component
Configuration Management Services	Limited	None
Capacity Planning and Performance	Medium	Metrics collection and reporting from new technologies: Helion Managed Private Cloud (MPC) and Helion Managed Cloud Broker (HMCB)

FRAMEWORK COMPONENT	EXTENT OF CHANGE	SPECIAL PROJECTS OR CONSIDERATIONS
Disaster Recovery Management Services	Large	Implementation of new architectures and addition of Business Continuity specialists to the support team
Identity and Access Management Services	Large	Modification of AD and ADFS architectures to support a single data center model, automation of Access Management Workflows to replace the CSRF form, IDAM transition, and PKI transition.
Reporting Management Services	Large	Implementation of the Service Portal and Data Analytics shall drive significant improvements in this area
Domain Name Management Services	Limited	None
Business Analyst Services	Medium	New Component
Chief Technology Architect	Limited	None
Enterprise Application Architect	Limited	None
Innovation Officer	Limited	None

The basic steps for developing the Cross Functional Component Management Plan shall be the same as those for creating new procedures. Upon County approval, the Cross Functional Component Management Plans shall be published on the Service Portal.

- Automated systems and tools involved in solution

Information feeds from various operational tools shall be used to provide Cross Functional Service deliverables.

No tools beyond those already described for managing the Transition process are required to transition the Cross Functional Framework.

E-Mail Services

- Description of solution to meet the requirements

Solution Summary

Contractor shall move the County to Office 365 Exchange Online.

Contractor shall work with CTO to identify the move groups, determine success criteria and finalize timing. Next, Contractor shall execute a proven HPE methodology, Migration Factory (MF). MF is a standardized service that uses specialized tools running on temporary servers to move email boxes from traditional Exchange servers to the Microsoft Office 365 Government Community Cloud. Contractor shall move County users in waves from Exchange to the MS Cloud over an 8- to 10-week period.

The email migration described above shall cover non-inbox PSTs that are in the current inbox. Contractor shall, in a separate PST Migration Project, migrate users' PST files to their Exchange Online Mailbox.

The PST Migration Project shall parallel that of the inbox migration and complete at approximately the same time.

Rationale

The Service Desk shall own tickets from start to finish in support of both Exchange and Office 365 environments.

This migration shall be accomplished prior to the end of the Transition Period, negating the need to upgrade the existing Exchange 2010 environment, allowing the data center based email infrastructure to be retired when the migration is complete.

- Deployment plan for resources and use of facilities

Members of Contractor's U.S. Messaging Practice, in coordination with CTO, shall both plan and execute the migration, with support from the local. A transition project manager shall guide the entire process, and County users shall be supported by the Contractor's Service Desk.

Contractor shall complete the migration virtually and at the Plano and Tulsa data centers. Microsoft engineers shall use the County ticketing system to support trouble tickets during the migration and provide experts to resolve issues if needed.

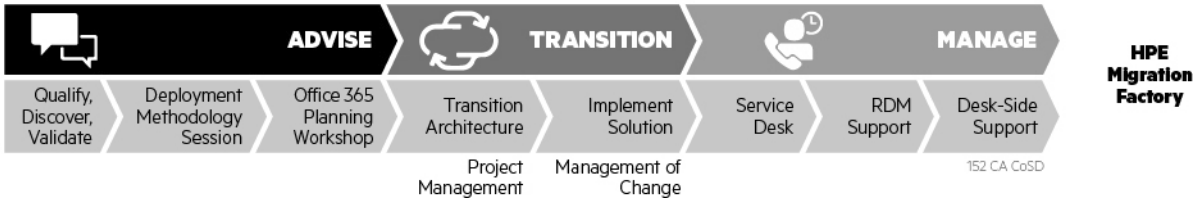
The County's Office 365 environment shall reside in the Microsoft Office 365 Government Community Cloud environment. This a hardened U.S.-based environment that is FedRAMP authorized, and whose support personnel are appropriately screened. It has features that can support Criminal Justice Information Services (CJIS) requirements for law enforcement agencies, and IRS-1075 requirements for customers who handle Federal Taxpayer Information (FTI).

- Key methodologies and processes in solution

Contractor's dedicated E-Mail migration practice shall be built on standard processes, tools, and trained personnel to assess, prepare, implement, and then decommission Exchange.

The Office 365 transformation methodology shall follow Contractor's standard advise, transition, and manage approach that closely follows the County's plan, build, operate formula (see figure below). Messaging engineers shall provide due diligence on the current environment, and prepare the infrastructure and tools that the Migration Factory personnel shall use to move from Exchange 2010 to Exchange Online.

Contractor's Advise, Transition and Manage Approach



Transition Schedule and Tasks

Contractor shall provide the final E-Mail Transition Plan and Schedule for County approval.

PST Migration shall follow a similar high-level methodology but with a simpler work breakdown. The basic process for PST Migration shall be as follows:

- PST Discovery: PST files are scattered among file shares and even local disk drives of End-Users. They shall be found via domain-level discovery of End-User shares and drives.
- PST Harvesting: Those files are then gathered in a central file store, linked to the End-User's Exchange Online account, and readied for import.
- PST Transfer: Whereas PSTs can be imported to Exchange Online via transfer over the WAN, for the large number of mailboxes and potentially large data sets, Contractor shall use Microsoft's Import Service via drive shipping. The data sets are stored on an encrypted drive and transported to Microsoft for import. This significantly reduces the amount of time for WAN transport of 15,000+ separate PST files.
- PST Import: Microsoft shall import the users' PSTs to their individual Archive Mailboxes. There is no size limit to the amount of emails that may be stored in Archive Mailboxes.

Plan and Design. For the Email Migration project, during the planning period, Contractor shall create the detailed migration plan and present it to the County for review and approval. As part of this process, the U.S. Messaging Practice, with advisement from the current email support staff, shall assess the environment, size the migration temporary infrastructure needs, and mitigate any potential or actual issues.

Configure. Contractor shall set up temporary infrastructure, configure the migration tool virtual server, configure DNS and network, and deploy a hybrid server. After system integration testing is successfully completed, Contractor shall perform a pilot launch.

Pilot Program. The Migration Factory shall perform a pilot migration on a subset of users defined by CTO, moving them to Office 365 and seeking feedback on their experience. Contractor shall conduct UAT in collaboration with the County, review results, and adjust Contractor's plan as needed based on the results and End-User feedback.

Documentation and Training. Contractor shall prepare service documentation, training materials, and Service Desk scripts to prepare for the migration waves. The County shall review the deliverables, Contractor shall respond to questions or clarifications, and then seek final approval to proceed. The completed documents and training material shall be added to the Service Portal, and Contractor shall train Contractor's Service Desk agents and other support personnel. Contractor shall review with CTO to determine if other types of training may be required and deliver that training accordingly.

Migration Waves. Contractor's Migration Factory shall then begin executing the migration move groups moving each group's mailboxes from the Exchange servers to the Microsoft Office 365 Government Community Cloud. Contractor shall complete the migration during an 8- to12-week period. As groups are migrated in waves, Contractor shall move into the manage phase, providing support.

Project Completion. Contractor shall request final County approval and sign-off. After all users are migrated and County approval is received, the E-Mail migration shall be complete. Similarly, after all PSTs have been migrated to users' archived mailboxes, the PST Migration shall be complete.

- Automated systems and tools involved in solution

To accomplish migration, Contractor shall provide and use Contractor internally developed software and a migration tool from Binary Tree Company. Contractor shall use a utility available from Microsoft for migrating PSTs.

Automated Tools

TOOL NAME AND VENDOR	DESCRIPTION
E2E by BinaryTree Corporation	• Analysis and migration engine for migrating on-premise Exchange mailboxes to Exchange Online • Allows rapid, low-risk migrations of large Exchange End-User populations. • This is the preferred tool of Contractor's messaging engineers
PST Capture	• Microsoft tool for searching and harvesting PST files

Development and Test Environment

- Description of solution to meet the requirements

Solution Summary

Contractor's solution for Dev/Test shall be tightly linked to the data center consolidation and the evolution of the Data Center to a hybrid environment: it shall use the Helion Managed Private Cloud (MPC), as described in the Data Center Consolidation Transition Project, and Helion Managed Cloud Broker (HMCB) to provide a business-rule defined boundary for Dev/Test capacity. This allows the environment's composition of server sizes and platforms in the hybrid environment to evolve and change over time in response to changing requirements without exceeding the County's established financial parameters. Contractor shall define thresholds to warn when the environment is approaching those limits.

Contractor shall provide a persistent Dev/Test environment for all P1 and P2 applications, so that high-priority County applications are guaranteed the resources needed to conduct testing in support of production issues (Applications Maintenance and Operations) or development projects. Contractor shall also maintain surplus space in the Dev/Test environment beyond that needed for the P1 and P2 applications to accommodate non-persistent Dev/Test capabilities for P3 through P5 applications. The surplus space shall be used on an as-needed basis to support the normal development and test activities of these lower-priority County applications. Contractor shall control the cost of the overall Dev/Test environment while also providing ample capacity for the County's suite of applications.

Contractor shall manage Dev/Test workloads within a SAN-based repository visible to the private cloud and perform tasks such as boot up and shutdown of virtual machine images on demand. Upon the County's request/approval, tasks shall commence. The Dev/Test environment shall have interfaces enabling connectivity to the Production environment to meet business needs. Contractor shall secure these interfaces with virtual local area networks (VLANs) and access control lists (ACLs). Identity access management services shall be applied across all County environments, including Dev/Test.

Contractor shall implement the HPE Codar toolkit to create an automated Release Management Framework in the Dev/Test environment. This shall support the evolution of Contractor's Applications Development Services to adoption of DevOps practices.

Rationale

Transition to MPC and HMCB shall provide an integrated platform for Dev/Test services that mimics the Production environment to streamline application development and deployment. HMCB shall provide the tools to create the hybrid design that the County is looking for in this environment. These tools provide the flexibility to include or exclude any type of platform within the Dev/Test scope, and manage its size based on a financial and business viewpoint instead of having to be concerned about the exact mix of

hardware and software. Contractor can make this definition all-inclusive or create the business rules to be less flexible according to the County's preference, without impacting the project timeline or plan. As the County's environment becomes more standardized, Contractor can collaborate to adjust the Dev/Test environment parameters to suit evolving requirements without reconfiguring the underlying technologies.

Because these tools are used to support applications in both Dev/Test and Production and are a key component of the Data Center Services Framework, transition of Dev/Test is designed to occur in conjunction with the remainder of the framework.

- Deployment plan for resources and use of facilities

The Data Center Consolidation Transition Project Manager (TPM) shall be directly responsible for activities associated transition of the Dev/Test environment. The Data Center Consolidation TPM shall be supported by the Cloud Services TPM, responsible for the MPC and HMCB services portion of the Transition. Contractor's virtual support team shall include architects, engineers, and migration specialists with expertise in cloud services and experience building out these environments for other clients.

The existing data center facilities in Tulsa and Plano shall support transition of Dev/Test until migration of all workloads is complete.

- Key methodologies and processes in solution

Transition Schedule and Tasks

Those tasks unique to the Dev/Test environment begin where Contractor configures the HMCB to establish virtual boundaries for the Dev/Test environment and other resource pools as needed. The preceding tasks are shown for context.

Planning and Build Phases. During the Consolidation Assessment task, Contractor shall build a migration roadmap detailing the placement, plan, design, and execution of migrations of development and testing workloads residing in Tulsa and Plano.

Once the hybrid architecture is built out, the Contractor's engineering and applications team shall collaborate with the County to define and size the composition of the Dev/Test portion of the environment, defining the financial parameters for each type of environment to be included. Dev/Test traditional servers already resident in Tulsa shall be included immediately; as servers from Plano migrate into the environment, they shall be imported into HMCB.

HPE Codar Environment Tasks. Once the Dev/Test environment is defined and built, Contractor shall design the environment for automated release management. This shall include design and configuration of the infrastructure, implementation of the software tools and necessary processes to manage them, and testing with a sample application.

Migration to Dev/Test. Contractor's migration engineers shall coordinate closely with the Application Development team to be aware of in-flight projects and migrate these at the proper time, in a non-disruptive manner.

Contractor shall prioritize move groups, with Plano workloads coming into Tulsa having the highest priority. This shall allow the County to consolidate into Tulsa as quickly as possible, to meet consolidation objectives. Contractor shall migrate all remaining non-production workloads into the Dev/Test environment (either by actual migration into the MPC or by including them in the virtual boundary created by the HMCB).

- Automated systems and tools involved in solution

Contractor shall use the same automated tools as described for, Consolidated and Single Data Center.

Consolidated and Single Data Center

- Description of solution to meet the requirements

Solution Summary

With the consolidation, Tulsa shall become the single production data center, and Contractor shall migrate all services from Plano to Tulsa. Contractor shall build a DR environment for the County at the Contractor's DR site in Colorado Springs, CO. It shall provide failover capability for applications that require DR, core services, and data center security services.

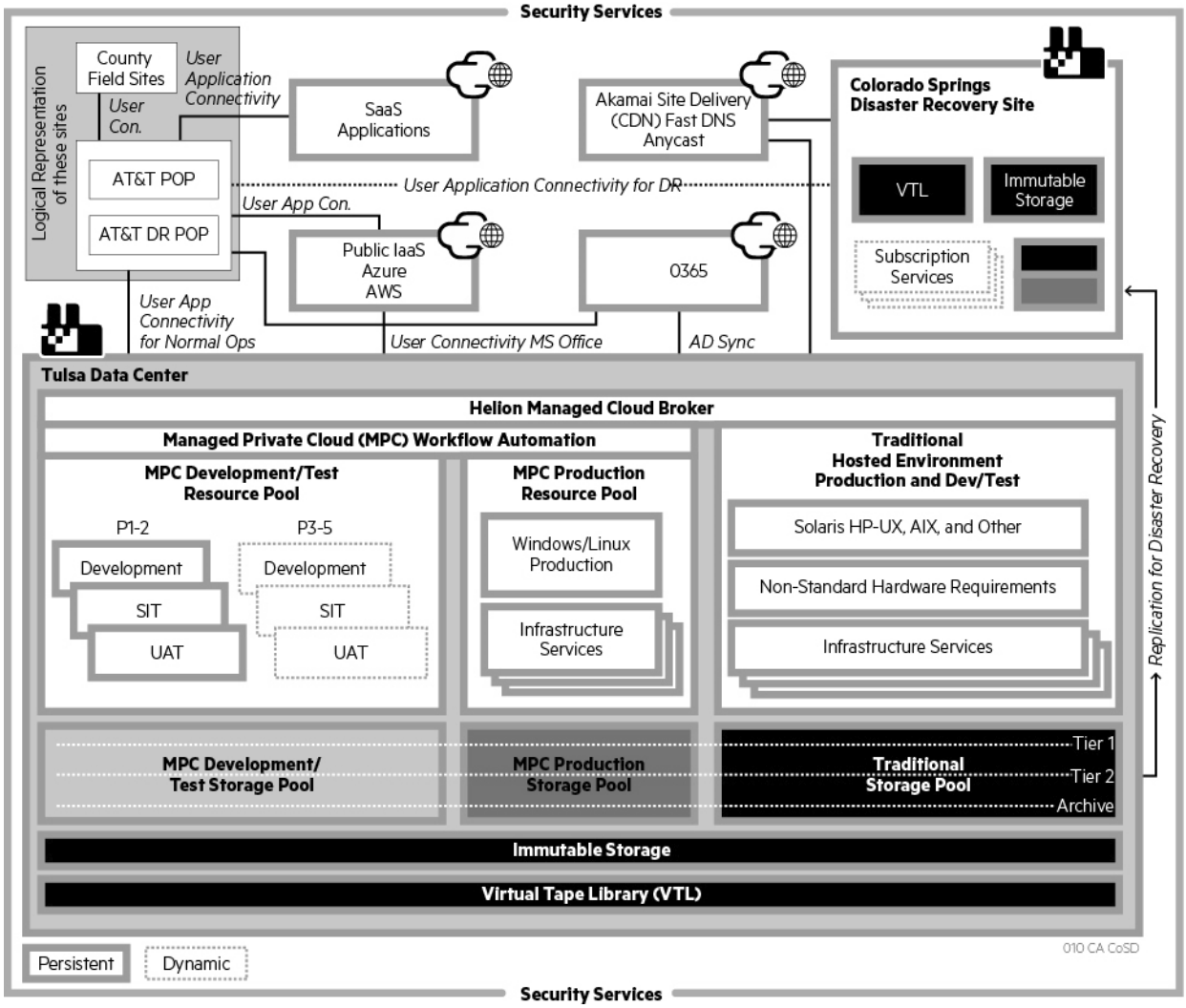
Contractor's structured transition approach for the data center consolidation shall be comprised of the following subprojects. These shall be completed in the sequence listed below to accomplish a smooth and non-disruptive transition.

- Set up and configure the data center network and security infrastructure to meet the new requirements.
- Refresh the data center storage environment to meet the requirements
- Build out the hybrid management capability and prepare the Tulsa data center to receive the server capacity currently resident in Plano. These activities shall be performed in parallel with the instantiation of the DR capability, and shall include the subproject to set up the development and test (Dev/Test) environment.
- Migrate applications, and in some cases, equipment, from Plano to Tulsa, based on a move group schedule provided by Contractor and upon approval by the County.
- Migrate the County's mail presence from the current Exchange environment to the Microsoft Azure Government instance of Office 365. Note that this project is not dependent on the ones above—it can be executed before or in parallel with them—but must be completed before the Plano environment can be decommissioned.

For each component identified above, Contractor shall provide a specific transition plan, interlocked with its related plan and the master schedule that details the tasks, milestones and schedule, for approval by the County. Throughout the project, Contractor shall work collaboratively with the County to develop success criteria, validate the scope and deliverables, and provide regular communication of the project's status, anticipated risks or issues, and Contractor's mitigation approach to make sure potential problems do not interfere with project completion.

The figures below provide an overview of the consolidated data center post-transition and briefly describe each component of the consolidated data center associated with the transition.

Consolidated Data Center Overview

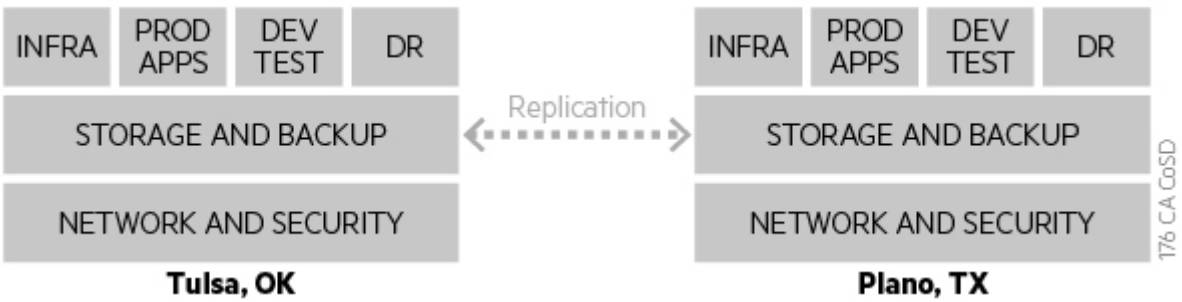


The Data Center Consolidation shall result in a modern hybrid environment.

Data Center Consolidation – Overview of Steps

The figures that follow describe the high-level steps for the consolidation project. The figure below depicts the County Data Center environment (Plano and Tulsa only), showing the basic classifications of servers and infrastructure as they are in place today.

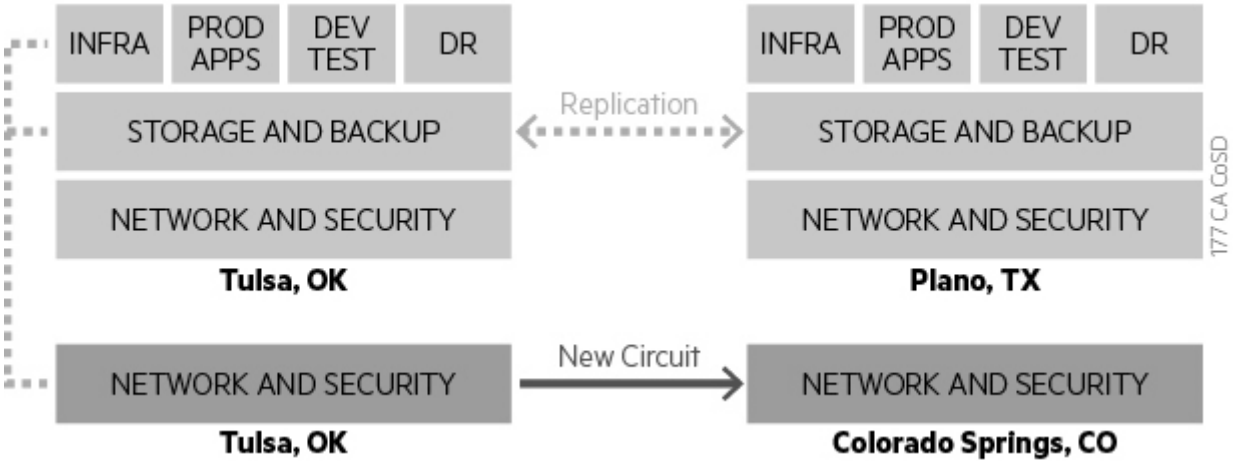
Current Data Center Environment



The first step, shown in the figure below, shall be to build out the new Data Center network compartment with the new network and security components. The new network compartment in Tulsa shall be built out in the same physical room as the current Tulsa environment. Its components are described in the second figure below. In parallel with the Tulsa network buildout, Contractor shall build out the network compartment for the DR environment in Colorado Springs.

The process to refresh/replace the network environment shall follow an "A/B" migration approach. Contractor shall build out the new network infrastructure (e.g., load-balancers, firewalls, switches, routers) reproducing the existing configurations on the new equipment. When Contractor has tested and verified the configurations, it takes a change window to shut down the "A" side of the environment (all traffic seamlessly fails over to the "B" side), and bring up the new equipment's "A" side. Contractor shall reroute the traffic to the new equipment and verify proper operation. Once Contractor is certain that no failback is needed, Contractor shall replace the "B" side of the equipment with the new equipment (again, in a controlled change window), re-test the failover, and once all is operating correctly, remove the old equipment.

New Network Compartments in Tulsa and Colorado Springs



Internet Connection. Leveraged Internet Service (LIS) provides shared Internet connections in a multi-tenant data center. Contractor shall obtain and manage the Internet connectivity to the data-center itself, and then extend that connectivity to applications in the data-center. Each LIS core router shall be connected (using link-aggregation) to both of the two WAN connectivity Layer-Aggregation Switches (WCL-AS) for the data center. Each LIS core router shall also terminate a connection from a separate ISP to provide diverse connections. The WCL-AS connections shall provide the path to the downstream LIS customer environment.

WAN Connectivity. The Contractor's data center shall be connected to the DR site using Ethernet MPLS WAN connectivity to provide high-speed data transmission, connecting back into the County's Points of Presence (POP). Connectivity shall be sized to 250Mbps of bandwidth with the capability to increase up to 1Gbps. Contractor shall have the capability of meeting any annual bandwidth increases should the County require. Within the Contractor's data center, Contractor's support team shall manage the dedicated WAN devices. Within the County POPs, Contractor shall ensure that AT&T manages the dedicated WAN devices. All network traffic between the data center and the POPs shall be encrypted.

The network design associated with the consolidated data center shall facilitate rapidly growing bandwidth and storage needs, reduce the complexity of the infrastructure, and deliver high availability (HA) and redundancy. This shall reduce the manually intensive processes and provide the convergence of networking and storage fabrics. It shall also contain standard 10Gbps and 1Gbps capabilities for attached devices, including servers, firewalls, and IPS devices.

The network shall provide a redundant topology to eliminate network downtime by a single point of failure. Contractor's network design shall provide redundancy for enhanced reliability with multiple connections to network devices. Network reliability shall be achieved through reliable equipment and network designs that are tolerant to failures and faults by reconverging rapidly to bypass faults when these occur. On a redundantly connected network, if a router fails, connectivity shall be preserved by routing traffic through a redundant connection. Furthermore, each router has two or more points, or "legs," to provide additional redundancy.

Contractor's design within the data center shall flatten the layer 2 architecture and provide a low cost capacity switching fabric. This shall be done through the adoption of a spine and leaf topology (2-tier) network design. The L2Spine is a high speed connection between any devices attached to the leaf nodes. It eliminates unused network links and introduces full throughput on all connections between network devices using Contractor's networking technology known as Intelligent Resilient Framework (IRF). Using IRF, multiple switches are grouped and appear as a single logical device that allows all links connected to these devices to forward traffic in a loop-free topology. Each device shall be fully redundant. IRF shall provide a non-blocking architecture within the layer 2 network fabric. It shall enable highly efficient high-bandwidth connectivity and N +1 redundancy. It shall provide up to 40Gbps of server connectivity to the access layer as the standard.

The data center network shall support the applications in Tulsa plus the applications that migrate from Plano. The migration moves a large amount of data across a Plano/Tulsa replication channel, but only at discrete points in time – it is not a continuous flow. Contractor shall provide the bandwidth required for each migration wave to ensure success. Contractor shall provide the bandwidth required for the Data Center consolidation, using diverse channels on the Contractor's Global Services Network (GSN) Transport. This is separate from the existing Plano/Tulsa replication circuits, and therefore has no impact on production replication traffic.

Disaster Recovery. The Tulsa data center shall be connected to the Colorado Springs DR site using a dedicated 10GB circuit, providing data replication for DR and off-site backup redundancy.

Once Contractor has tested the new network, Contractor shall cut over all the current connected equipment, as depicted by the dotted lines in the figure below. This shall be done in a planned change window, and shall be transparent to the County because all components are redundant.

Storage Architecture.

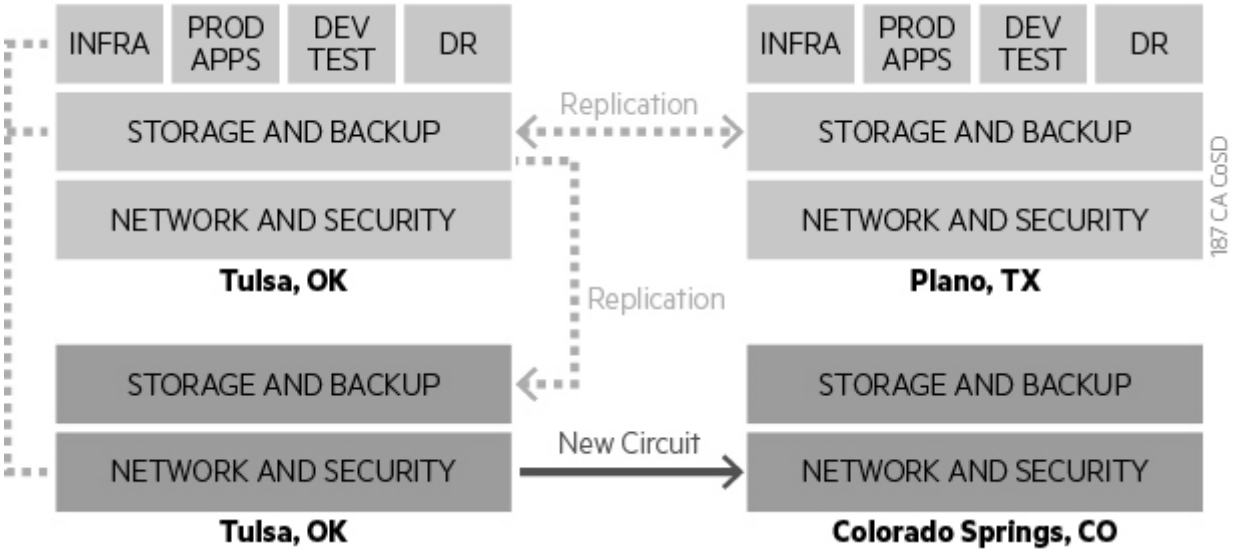
The figure below provides a view of the refresh of storage requirements:

Site	Refresh point
Tulsa (SAN, Immutable, VTL)	Transition
Colorado Springs (SAN, Immutable, VTL)	Transition
View Ridge & Lemon Grove (SAN)	Storage Refresh Schedule
AT&T POP (SAN)	Storage Refresh Schedule
DR POP (direct-attached only)	Server Refresh schedule

Rancho Bernardo (SAN, VTL)	Storage Refresh Schedule

The next step shall be to build out the new storage and backup equipment in Tulsa and Colorado Springs (Rancho Bernardo and other DPC sites shall have their storage refreshed on the normal refresh schedule), and start synchronizing the data between the current storage array and the new one, as shown in the figure below.

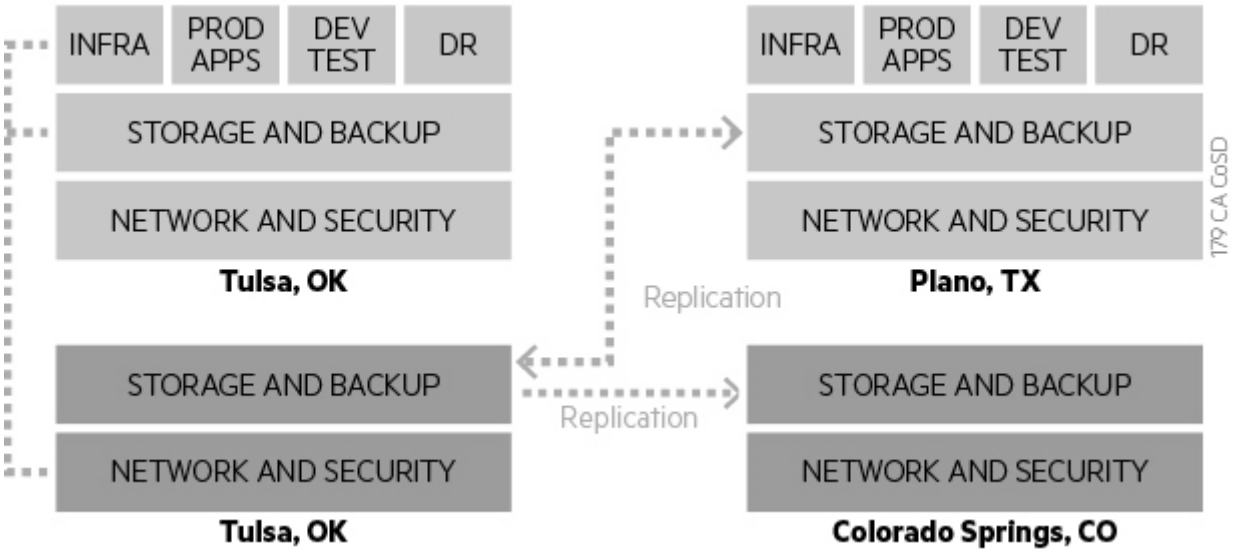
Deploying New Storage, Migrating Data



Once the new storage is fully synchronized with the current production array, Contractor shall cut over the SAN connectivity, re-initiate the replication between Tulsa and Plano, and replicate the DR data to Colorado Springs, as shown in the figure below.

In order to avoid migrating End-Users' Home drive storage twice, the County may wish to migrate this data to OneDrive for Business (ODfB) as defined in the User Data Services Transformation Project prior to the storage migration. Contractor shall accommodate this request, provided that the County can commit to supporting Contractor in achieving the ODfB migration in 6 months or less from CED (the currently planned schedule calls for 7 months), with larger move groups. If the project cannot be completed in that timeframe, Contractor and the County shall permit the Data Center consolidation to proceed on schedule anyway (i.e., do not create a dependency between the two projects) in order to avoid the risk that the Data Center Framework Transition exceeds its allowable timeline due to delays in the OneDrive migration

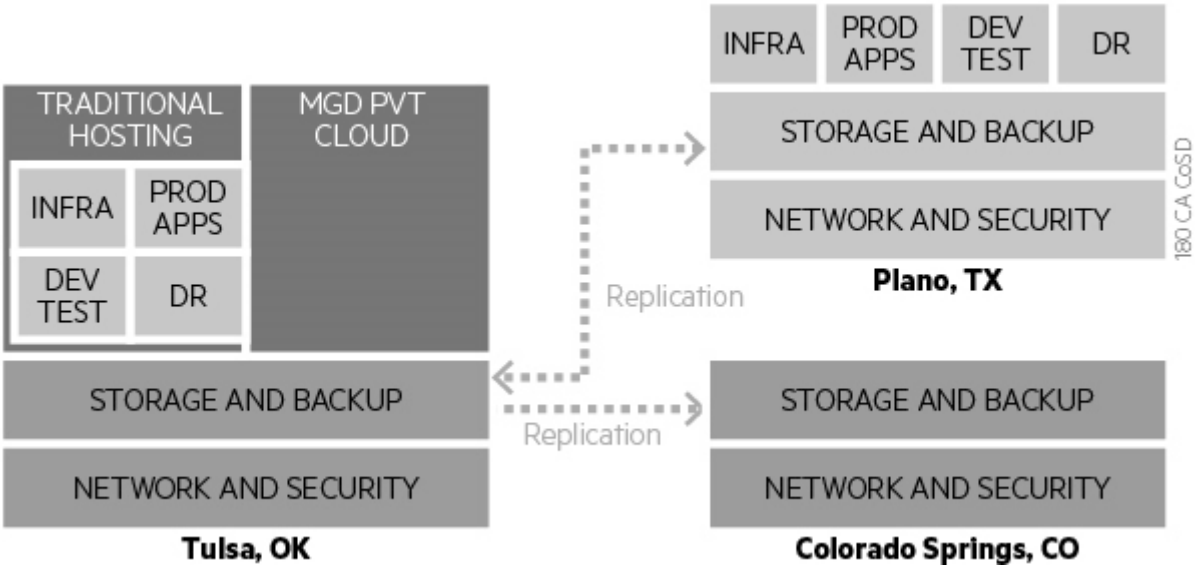
Cutover to New Storage Arrays



Then Contractor shall decommission the old storage and network environments (see figure below).

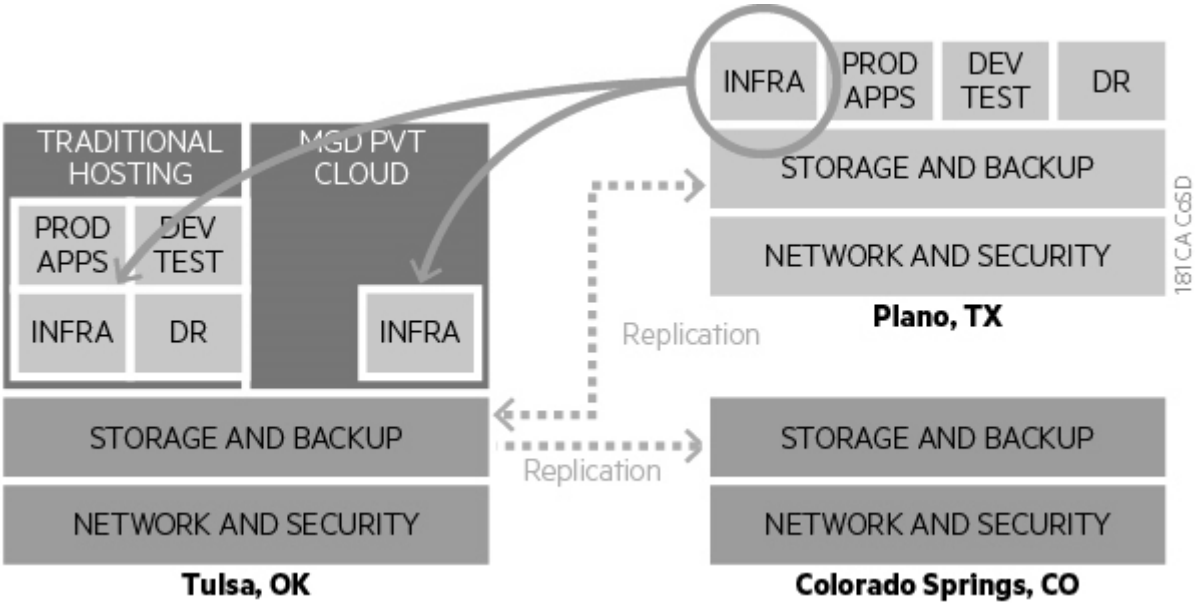
At this point, no migrations have taken place: Contractor has built out the new capacity to support the migration and the hybrid cloud architecture.

Decommission Legacy Network and Storage Hardware in Tulsa



Contractor shall build out the MPC—the County's pre-configured cloud resources—while the migration planning and detailed scheduling is taking place (see figure below).

Migration from Plano to Tulsa



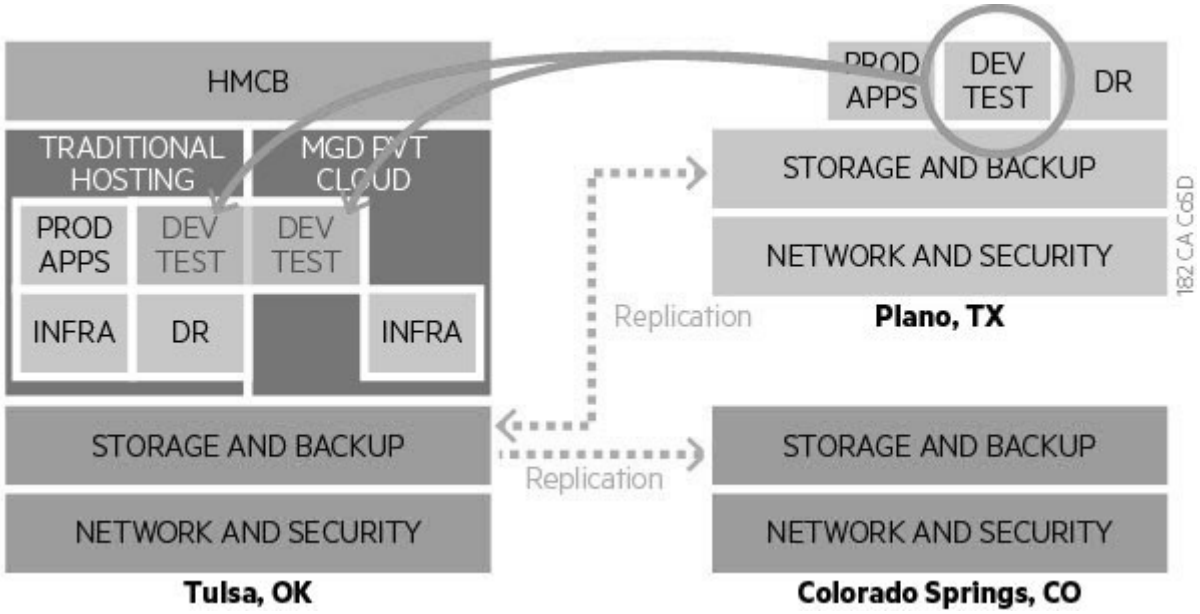
Data Center Hybrid Architecture. Contractor shall deploy hardware and software for a hybrid computing solution that supports applications and infrastructure services for the production and Dev/Test environments. The hybrid architecture shall combine a HPE Helion Managed Private Cloud (MPC) for cloud-compatible applications and traditional hosting for business applications that are not cloud-compatible, resulting in a hybrid environment. The MPC and the traditional hosted infrastructure shall accommodate the combined workloads from Plano and Tulsa, and shall be able to scale as needed to support the County's needs.

Servers with resource needs higher than the predefined sizes can be migrated into the largest size, then scaled up to meet their resource needs. Sixty percent of the servers in the data center environment are already located in Tulsa and technically do not have to move to achieve the County's consolidation goal; however, to gain the benefits of automated provisioning and the ability to turn servers up and down for Dev/Test and Applications M&O "Break/Fix" environments, Contractor has included the cost of moving those that are eligible to be hosted in MPC during the Data Center Transition, to include application regression testing. Sixty-seven percent of the servers in both Plano and Tulsa are eligible to migrate into MPC; however, per the County's request, Contractor shall not migrate the Tulsa production servers during Transition.

Contractor shall work with the application stakeholders' users to identify the best migration windows and methods for each application or related group of applications, and, depending on the platform, Contractor shall either migrate them into the Traditional hosting environment or into the MPC, as depicted in the figure below.

Building out the Cloud Broker shall take place in parallel. As Contractor creates the pool view of the Dev/Test environment, Contractor shall migrate servers from Plano into it, and either keep them live if they are P1/P2 applications or traditional infrastructure, or turn them down if they are P3-P5 in MPC and are not currently being used for a project or active M&O work. See figure below.

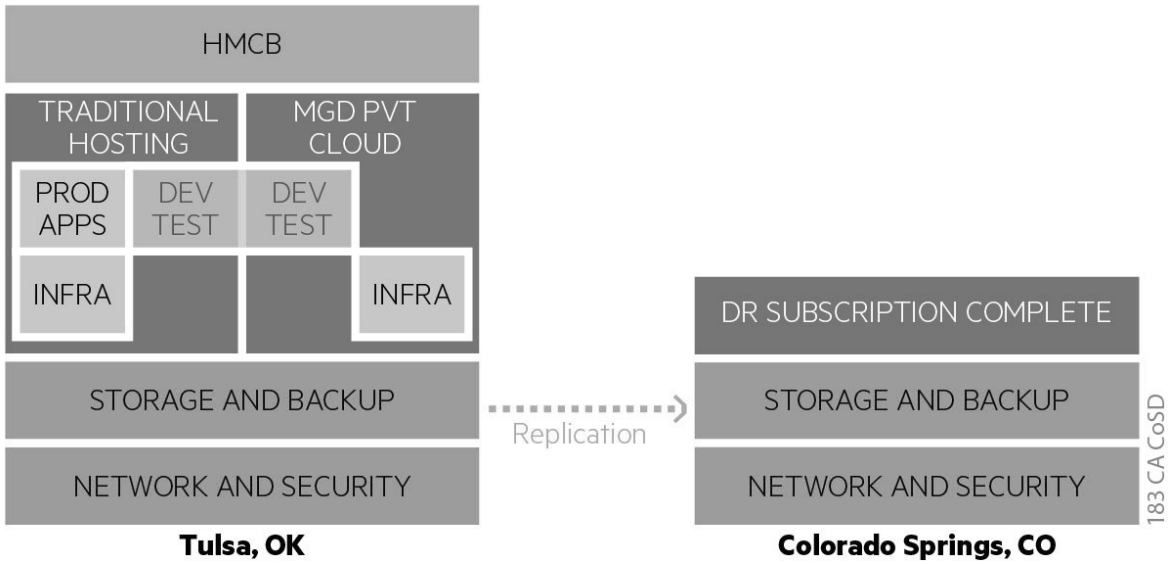
HMCB Deployment, Establishment and Migration into Resource Pools



As Contractor moves the production servers, Contractor shall make sure that their corresponding DR subscriptions are in place before the migration move group executes. That there shall be minimal changes to applications—only what is needed to facilitate the migration and redirect any Internet access from using the County's Internet at the COC and POP to the Leveraged Internet Service.

Once the migration from Plano is complete (or in parallel, as schedules permit), Contractor shall move any eligible Test and Development environments in Tulsa into the MPC. As shown in the project schedule, the migration plan and pricing include moving any eligible Tulsa server environments into the MPC; however, these moves can be deferred to the refresh timeframe, if this is the County's preference.

Future Mode of Operations



The mainframe and AS400 environments shall need to remain intact beyond the end of the Transition period. The infrastructure required to support those environments shall remain in Plano for as long as those systems are needed.

Rationale

Contractor shall enable multivendor support across hypervisors, OS instances, and infrastructure. Contractor shall provide a private cloud environment that consists of server, storage, and networking built for the cloud. It shall also consist of security, automation, and management software designed for hybrid delivery.

Contractor shall consolidate the data center workload that is currently hosted in the Contractor's Plano, Texas data center facility into Contractor's Tulsa, Oklahoma facility.

Contractor's Cloud Broker solution shall provide the County with an enterprise view of all data center platforms, including private cloud, public cloud, and traditional hosting environments. The cloud broker shall give the County the ability to have an enterprise view of system performance as well as financial management across each of the hybrid platform through one pane of glass. It also shall provide a single console for provisioning compute resources across the County's hybrid estate.

- Deployment plan for resources and use of facilities

Contractor shall assign a data center consolidation transition project manager (TPM) that shall report to the Transition Services Manager. The TPM shall have overall responsibility for this project and shall be the primary point of contact for the County in support of all data center consolidation activities. This TPM shall be responsible for maintaining the Contractor's Move Group Plan and collaborating with the County's designated project leader, as well as coordinating activities with the other TPMs and the Contractor Project Management Office. Contractor shall also assign a Contractor account executive sponsor to provide executive visibility throughout the project.

The data center consolidation TPM shall be directly responsible for all activities associated with the DR and storage architecture subproject activities and provide oversight of the team. The TPM shall be assisted by:

- Another TPM that shall be responsible for the buildout and testing of the cloud components
- A TPM whose focus is applications readiness, and shall work closely with the County and the Contractor team to closely manage application testing, remediation (if necessary), and scheduling priorities of the County stakeholders.

Contractor's virtual support shall include architects, engineers, and migration specialists with specialized expertise in each of the disciplines required to deliver the various components of the plan.

The data center facilities at Tulsa, Plano, and Colorado Springs shall support transition. The transition project management teams shall be headquartered at Contractor's Rancho Bernardo site.

- Key methodologies and processes in solution

Transition Schedule and Tasks

As described above, Contractor shall use a phased transition approach to accomplish the data center transition. For each phase, Contractor shall follow a standard process that includes an assessment of the existing environment to adjust for any changes that may have occurred as of the Contract Effective Date and the status of any in-flight projects. Each phase of the plan shall include submission of project deliverables to the County for review, response, and subsequent approval, and all approved project deliverables shall be made available to authorized users via the Service Portal.

Because the data center transition has a number of interdependencies and subprojects, Contractor shall first initiate a planning and governance phase, as part of the overall transition high-level planning sessions, which shall kickoff this set of projects.

Consolidation Assessment. In preparation for the migration of the applications from Plano, Contractor shall classify servers in terms of their migration targets and analyze server mapping.

Following the high-level planning activity, Contractor shall move directly into the detailed design and build phases. The first part of the implementation is the data center network. The draft data center network transition plan is depicted in the second figure below. An early output from the assessment shall be identification/verification of additional network bandwidth needed in the Tulsa data center. Contractor shall use this information to engineer the new network design and identify the specific network devices and configurations to be ordered and installed in Tulsa. Contractor shall submit this plan to the County for approval prior to placing equipment orders. Once approved, Contractor shall develop the final Bill of Materials and order the equipment.

With receipt of the equipment, Contractor shall begin installation of the data center network compartments in both Tulsa and Colorado Springs. In the Tulsa environment, Contractor shall create interconnects between the existing and new network infrastructure, then reroute traffic to the new or upgraded circuits. An integral part of the new network architecture is the establishment of the firewalls/IPS' and security zones needed to support traffic segregation and authorized third-party access. As part of the overall testing process, Contractor shall validate and test third-party access to the new network environment. Once testing is successful, Contractor shall move the network design deliverables to "as-built" documents, update all process documentation based on the new technologies, and submit all required deliverables to the County for review and approval.

As the network design and buildout is taking place, Contractor shall analyze the DR requirements.

As part of the Data Center Consolidation transition design process, Contractor shall seek to optimize County software licensing costs. Existing County software has a variety of licensing models such as site/enterprise, concurrent user, named user, module, managed budget, server, CPU, and core. Licenses based on server, CPU, and core present an opportunity for consolidation and license cost savings. Examples of County vendors that use these types of licensing models for enterprise server software include Adobe, EMC, Microsoft, Oracle, Symantec, IBM, and VMware.

Methodologies to reduce license obligations for server/CPU/core based licenses include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated to headroom at each site versus single site's shared environment.

MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases.

Data Center Services DR Plan and DR Architecture Implementation.

During the design phase, Contractor shall review the environment specifications for the Disaster Recovery site, and shall make any updates needed. The final specification shall be conveyed to the Colorado Springs team, who shall put in place any necessary hardware and software to support the subscription contract.

Once the network connectivity between the Tulsa and Colorado Springs is established, Contractor shall begin replicating both live data and virtual tape library (VTL) data and verify that data replication is occurring accurately and as planned. At the end of the phase, Contractor shall perform three tabletop exercises of the DR plan to validate its functionality and address any deficiencies found during the exercise. Following successful completion of these exercises, at least 90 days prior to the cutover date for the data center framework, Contractor

shall submit the draft DR plan for framework to the County for review and comment. Once Contractor has at least a few applications running in the Tulsa environment, Contractor shall schedule an actual failover test. Using the HPE Helion team's established DR testing methods, Contractor shall be able to conduct a failover test without forcing an actual outage to the production applications.

Data Center Hybrid Architecture and Consolidation to Tulsa

Consolidation Assessment. As described above, Contractor shall assess the Plano application and infrastructure environment to identify the migration approach for each. Contractor shall prepare a source-to-target mapping that documents each of the servers that shall be migrated along with the target server characteristics during this stage. Contractor shall also do an assessment of application requirements to the services provided by the MPC to determine compatibility. If there is a match, the application's Dev/Test and/or Break/Fix servers shall be moved into MPC. Contractor shall work collaboratively with the County's business users to determine the most appropriate solution for each application. Contractor's applications team shall review the applications targeted to migrate to verify if they have any common issues that need to be mitigated prior to migration, such as hard-coded IP addresses. If Contractor discover any issues, Contractor shall mitigate them prior to migration, using established change control procedures. From this process, Contractor shall have a clear picture of where Contractor needs new equipment and where Contractor has opportunities for reuse and for migration using a pack-and-ship approach, and can refine and adjust the target server environment solution into a design that reflects the detailed configurations.

Design and Procure Target Server Environment. Contractor shall design the hybrid environment in Tulsa to include:

- MPC and Cloud Broker (HMCB)
- Expansion of the capacity of the existing traditional infrastructure in Tulsa to accommodate workloads from Plano that require traditional hosting.

From the completed design documents, Contractor shall develop Bills of Materials and engineering documents, and submit internal purchase orders for any new hardware and software required. There shall be no additional cost beyond the Transition price for this activity.

Design Migration Plan. During the design phase, Contractor shall also identify move groups that shall organize the servers according to application dependencies, and incorporate other critical factors such as the change "freeze" periods, allowable maintenance windows, and other business priorities. Contractor shall migrate all applications supporting a business process together when possible rather than migrating individual applications. Contractor shall assign a work packet for each server group supporting the same application, which shall be combined into move groups based on the critical factors identified above and application resource availability. Contractor shall create a consolidated move group plan that Contractor shall present to the County for approval.

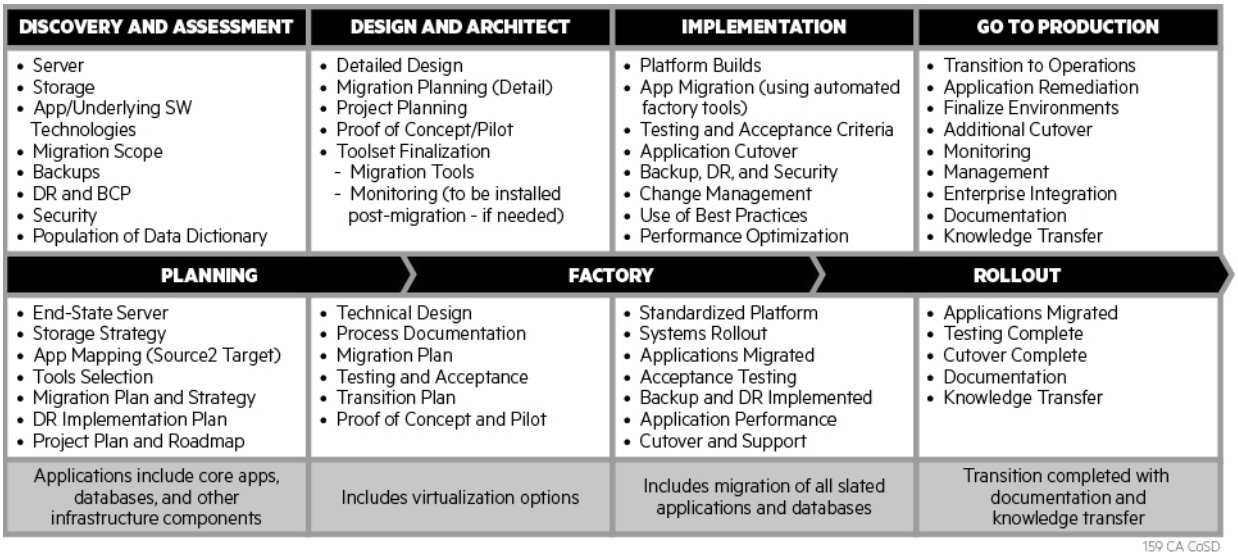
Build-Out Hybrid Environment. The build-out of the hybrid environment shall include installing new racks, power and cabling, installing, and configuring the MPC and traditional hardware and software. Contractor shall also install and configure the HMCB. Contractor shall perform tests on the newly built servers to verify that automation processes as well as traditional connectivity and configurations to existing back-end management and reporting systems are in place, then create or update documentation for the target systems. Note that the storage architecture shall have been built out under a separate but integrated plan: at this point in time, the two schedules converge. Once the build is complete and tested, Contractor shall begin migrating move groups over the network. Tasks to build out the Dev/Test environment capabilities shall also commence during this phase.

During this time, Contractor shall work with County application stakeholders to create the detailed Migration Plan and other sub-deliverables, such as the Back Out plan, and determine the change window to execute the go-live. During this phase, Contractor shall work with and provide guidance to the County to plan the tasks and secure

required resources to successfully execute the Migration Plan. Contractor shall also begin the necessary change management steps and communications processes in conjunction with the County.

Execute Migration Move Groups. An overview of the Contractor's migration methodology phases is provided in the figure below.

Migration Factory Methodology



Adherence to this methodology shall enable Contractor to deliver a flawless data center consolidation.

During the assessment and design phases of the project, Contractor shall build a migration roadmap detailing the placement, design, and execution of workload migration of all workload residing in Plano and Tulsa to achieve the consolidation. Contractor shall prioritize workload migrations, with Plano workloads into Tulsa taking the highest priority. This shall allow the County to consolidate into Tulsa as quickly as possible to reduce the cost and complexity of operating in two data centers.

Pack-and-ship migrations may begin before the hybrid environment buildout is complete, if permitted by the County. If Contractor is able to ship servers before the Broker is in place, Contractor shall import those systems to the governance facility once the Broker is live to make them part of the hybrid environment.

Migration activities shall follow step-by-step processes for the Dev/Test and production environments. During this phase, Contractor shall work with the County, Contractor's technical resources, and Contractor's application SMEs to execute the migrations from the source to the target environment. The migrations shall be in accordance with the approved Migration Plan and approved detailed design documentation according to the migration schedule for each move group. The contents shall be captured in the Migration Plan developed for each application. Tasks performed as part of the Go-To-Production process, such as executing hardening scripts, loading software agents for antivirus and adding the devices to the central repository, are incorporated into the project plan to make sure that the approved Go-To-Production process is followed for all migrations.

During the migration, as assets migrate, their Resource Units shall be recast to the billing structure of this Agreement. The County shall not be billed for both in the same month.

Contractor's migration engineers, with the support of the County-designated project manager and application and infrastructure SMEs, shall execute the Migration Plan according to the project schedule. The business owner of

the application shall provide the final approval during the cutover and is responsible for coordinating End-User acceptance testing and declaring the migration a success.

All migrations shall have contingency plans to invoke a back-out or other service restoration procedure in the event of a failure, or a scenario where the migration is at risk of exceeding its allotted window. The County business owner must approve any criteria for invoking the contingency plan as well as the execution of any contingency plan.

The migration plan shall include County freeze periods and adjust migration move groups accordingly, and shall consider migration alignment with maintenance windows to minimize downtime. Migration of applications impacting critical services shall be reviewed; upon County approval, Contractor may invoke the contingency plan to mitigate impact on critical service supporting County business. Each move group plan shall require County approval and participation by the application stakeholders in acceptance testing.

Automated tools like DoubleTake and PlateSpin shall help mitigate or lower the downtime considerably, as migration can be performed while source servers are live: stakeholders can test on the target servers at a time convenient for them in most cases.

- Automated systems and tools involved in solution

Contractor shall provide the migration tool licenses, such as DoubleTake and PlateSpin. Some applications may be manually installed into the target data center Following the initial seeding, the County application team shall test the application in the target data center.

Contractor's Migration Factory shall use a tool from Binary Tree Company. Contractor shall execute multiple move groups concurrently, consisting of multiple applications and associated components and using software products such as those described in the table below.

Automated Tools

TOOL NAME AND VENDOR	DESCRIPTION
DoubleTake	DoubleTake v7 is a migration tool that shall be used for migration from Plano to Tulsa. DoubleTake performs a complete server copy from the source server onto the target server. It also has an advantage of having an asynchronous replication feature, significantly simplifying the data synchronization effort required during the final go-live process. Data synchronization can be set to certain files, directories, or file systems, optimizing the amount of data being transmitted on the network.
PlateSpin	PlateSpin v11 is a migration tool similar to DoubleTake and shall be used for migrations into the County managed private cloud. PlateSpin performs a complete server copy from the source server to the target server, if needed. It allows source servers to be copied as an image that can be transported using an approved portable storage device and then restored to either a physical or virtual server on arrival at the Tulsa data center.

Storage Architecture

- Description of solution to meet the requirements

Solution Summary

The core of Contractor's primary Data Center Storage Architecture shall include the latest innovation of HPE 3PAR enterprise storage, which is designed for both cloud and traditional environments. The storage shall host operating system images, virtual snapshots, and application data. Contractor's architecture shall enable the server

image to be disassociated from the physical hardware, allowing the image to move from one physical server to another as needed for greater flexibility, better resource utilization, and built-in failover.

The table below summarizes the types of storage in place in the County as of the Contract Effective Date, the migration technologies in use for each, and the Transition strategy for each.

Storage Transition Summary

TIER	AS OF CED	FUTURE	TRANSITION APPROACH
1 (Data Center)	3PAR P10000 thick provisioned 15,000 RPM drives (Plano and Tulsa)	3PAR P20000 thick provisioned 10,000 RPM drives (Tulsa)	Replication, Peer Motion
1 (AT&T POP)	3PAR StoreServ 8400 2N Solid State drives	3PAR StoreServ 8400 2N Solid State drives	No change in Transition. Contractor shall review and re-address the architecture when this storage comes due for refresh.
2	3PAR P10000 thinly provisioned 15,000 RPM drives (Plano and Tulsa)	3PAR P20000 thinly provisioned 10,000 RPM drives (Tulsa)	Replication, Peer Motion
Archive	3PAR P10000 thinly provisioned 7,200 RPM drives (Tulsa)	3PAR P20000 thinly provisioned 7,200 RPM drives (Tulsa)	Replication, Peer Motion
DPC	3PAR 7200 with 10,000 RPM drives	3PAR 7200 with 10,000 RPM drives	No change in Transition. Contractor shall review and re-address the architecture when this storage comes due for refresh.
Immutable	EMC Centera SN4	EMC Centera Gen4LP	Replication
Email	Email is stored on the 3PAR in both Plano and Tulsa	Provided by the Microsoft Azure Government Cloud	E2E Complete™
Mainframe	HPE P9500 or equivalent in Plano (leveraged)	HPE P9500 or equivalent in Plano (leveraged)	None. Mainframe storage remains intact until the mainframe is decommissioned. At that time, the new midrange solution for those applications that have been deployed (under a separate project) using the appropriate tiers of SAN storage.
Direct-Attached	Disk drives installed on and dedicated to a physical server (types may vary)	Disk drives installed on and dedicated to a physical server (types may vary)	None specific to the storage environment. Direct attached storage shall be replaced, and its data migrated to new storage at the time its associated server is refreshed.

TIER	AS OF CED	FUTURE	TRANSITION APPROACH
Backups (Data Center)	HPE StoreOnce B6200 Virtual Tape Library (VTL)	HPE StoreOnce B6600 Virtual Tape Library (VTL)	Replication
Backups (DPC)	HPE StoreOnce D4212 at Rancho Bernardo MSL 4048 Tape Library	HPE StoreOnce D4212 at Rancho Bernardo Replicating to DR site in lieu of tape creation, for offsite storage	No Transition of VTL environment; only need to start replication to Colorado Springs Tape Libraries shall remain intact until all tapes are expired.

The 3PAR 20000 is the latest innovation in enterprise storage from HPE. Primary data (all 3PAR-based tiers) for applications with a 48-hour Recovery Time Objective (RTO) is replicated to the DR site. The primary immutable storage shall be located in the new production data center in Tulsa on refreshed EMC Centera storage and shall be replicated to a refreshed Centera at the DR site. Contractor shall refresh the 3PAR storage at the County's San Diego sites with like 3PAR storage to reduce the impact on operational processes and maintain the same level of performance. The backup solution shall meet the requirements by providing a refreshed StoreOnce VTL in Tulsa and a smaller refreshed StoreOnce in Rancho Bernardo, both replicating to the DR site for remote storage of backup data. The backup solution changes from the current solution by replicating all data center backup data to the DR site and by eliminating remote offsite storage of backup data on tapes for the Rancho Bernardo site in favor off replicating that data to the DR site as well.

Rationale

Contractor shall meet the increased capacity and transaction requirement of the consolidated data center environment and improve the storage architecture for primary SAN storage, Contractor shall transition to a refreshed, dedicated SAN with a 3PAR 20000 storage array.

Contractor shall provide improved storage performance and capacity at the point of refresh, without disruption to County business applications. Contractor's Transition shall ensure data redundancy between Plano and Tulsa is re-established in the Colorado Springs DR site prior to removal of the Plano environment.

- Deployment plan for resources and use of facilities

Depending on the type of storage and stage of the Transition, Contractor shall execute this project at the Tulsa and Plano data centers and Contractor's Rancho Bernardo site.

Contractor's storage Transition engineers shall come from Contractor's U.S. Public Sector delivery organization, a virtual team composed of U.S. citizens based in the Continental United States, working in close coordination with the local San Diego teams.

Contractor shall engage EMC Professional Services to install, configure, and migrate the existing immutable storage environment to the refreshed environment.

- Key methodologies and processes in solution

Contractor shall use a combination of host-based and storage-based replication to migrate data to the new storage and backup infrastructure without interruption to business processes and without data loss.

Transition Schedule and Tasks

Contractor shall adjust the schedule based on the final detailed plan.

Plan, Procure, and Engineer (Design). Contractor shall create a detailed plan and design for the new storage architecture and provide engineering documents to migrate data from the original storage solution in Plano and Tulsa to the new storage solution in Tulsa and Colorado Springs (DR). Contractor shall submit the design and plan deliverables and review them with the County. The County shall review and respond based on the agreed schedule. Contractor shall make any final revisions and create the detailed Bill of Materials from which Contractor shall procure the needed hardware, software, and services. All design deliverables shall be posted to the Service Portal as required.

Build New Storage and Backup Architecture, Enable Remote Replication. Once hardware is received, Contractor shall begin the build process. Contractor shall install the new SAN switches, storage, and VTL in Tulsa, configure and test the environment, and begin the process of replicating data from the current Plano array and VTL to the new Tulsa array and VTL. Contractor shall replicate from Plano to Tulsa throughout the Data Center Consolidation project, and replication shall be shut down for each application at the point during the consolidation when all application data has been verified and accepted on its Tulsa system.

Preparation of the DR environment shall also occur in parallel with the buildout at Tulsa. Once the DR environment is available, Contractor shall begin replication of SAN storage for applications that require DR with a 48-hour Recovery Time Objective (RTO), from the new Tulsa array to the DR site. Contractor shall replicate VTL data to the DR site for applications that require DR with a 72-hour RTO. Contractor shall begin replication of VTL data from Rancho Bernardo to the DR site for offsite storage.

Contractor shall engage EMC Professional Services to perform the Transition activities for Immutable Storage; this shall include refreshing both Centera units. The new units shall be located in Tulsa and in the Colorado Springs DR site. The new Tulsa Centera shall be configured to take over as the primary, and shall replicate to the Centera at the DR site. All existing Centera data shall be replicated to the new Tulsa Centera. The Centera refresh/migration shall not require downtime. Contractor shall reboot the Centera shortly after refresh/migration. The reboot process shall cause about one hour of downtime for the immutable storage service environment. Contractor shall coordinate this activity, like all Transition tasks, with the County via the Change Management process.

The rest of the Document Processing Center (DPC) storage and backup architecture shall be refreshed at the appropriate time post-Transition—there are no tasks required during the Transition period.

Migrate Local Data – SAN. Once the new SAN and Backup environment are fully configured and ready to support live servers, the various migrations described in the Consolidated and Single Data Center section shall begin. In addition to supporting these migrations, servers that are not migrating (that sit in Tulsa currently) shall also have their storage migrated to the new environment. There are no dependencies between the Data Center Consolidation and migration of the current Tulsa servers to the new storage—these two activities can occur in tandem.

To migrate the Tulsa environment to the new storage, Contractor shall first verify that all data is fully synchronized from the existing array. The SAN has redundant connectivity, and Contractor shall take advantage of this redundancy to move the environment from the current to the new SAN without requiring an outage to the systems or applications. Contractor shall move one set of connections from the current fabric to the new fabric, switch data access to the new fabric, then move the second set of connections to the new fabric. Contractor shall then enable replication of these volumes to the DR site.

In the new storage architecture, End-User data storage shall be provided directly from the new NAS-capable 3PAR, eliminating the need for NAS appliances. This change shall be transparent to the users.

As previously noted, Contractor and the County shall strive to migrate End-User data to OneDrive for Business in order to avoid having to migrate it to the new array as well. If the End-Users cannot commit to the four-month timeframe required, and the County does not wish to elongate the timeframe for the Data Center Framework

Transition, Contractor shall build out the End-User NAS shares by providing End-User data storage directly from the new NAS-capable 3PAR, eliminating the need for NAS appliances. This change shall be transparent to the users.

Following successful completion of the Storage Architecture Transition, Contractor shall securely destroy all data on the retired storage and backup systems and provide disposal of those items.

- Automated systems and tools involved in solution

Both the backup storage (VTL) and 3PAR shall have native replication capabilities built into and enabled by the storage array software. When host/system-based replication is used, DoubleTake V7 shall be the tool that migrates the data along with the server image. The following table lists storage-based tools and utilities.

Storage-Based Tools and Utilities

TOOL	DESCRIPTION AND USAGE
VTL Utilities	StoreOnce replication using Catalyst Replication of de-duplicated backup data reduces time and bandwidth on the dedicated replication link between Tulsa and the DR site. Backup data is available for DR more quickly, to reduce the chance of missing backup data in case of a DR event.
3PAR System Utilities	• 3PAR array-based replication allows background replication of storage from one array to another and shall aid the migration of service data from Plano to Tulsa. • 3PAR Storage Peer Motion allows Contractor to migrate storage data volumes off the old Tulsa 3PAR onto the new Tulsa 3PAR without any interruption in accessing the data.

Service Portal

- Description of solution to meet the requirements

Solution Summary

Contractor's End User Access (EUA) solution, integrated closely with Contractor's Service Management systems (Service Manager), shall provide a centralized Service Portal for all County users. Contractor's Service Portal shall provide access to self-service assistance options and multiple dashboards easily accessible by County users, Service Desk agents and Contractor support teams. It shall be mobile-enabled and easy to use.

During the Service Desk Transition, which shall occur in accordance with the Transition schedule, Contractor shall set up the core Service Portal functionality, including single sign-on, and link it to current data sources and source systems to integrate with the current repositories.

- Deployment plan for resources and use of facilities

Contractor shall assign a TPM for the Service Portal Transition Project. Contractor shall work with the County Technology Office (CTO) and its designees to assist in the design and testing and governance of the Service Portal. Contractor's Global Engineering and Technical Consulting (GETC) organization shall provide the engineering and customization work, in collaboration with the County's local engineering and support team, which manages the current portals. Contractor shall hold design sessions with the County at Contractor's Rancho Bernardo site or at a designated County location.

- Key methodologies and processes in solution

Contractor shall use infrastructure project management processes in delivery of the project.

Transition Schedule and Tasks

The following figure provides a sample view of the activities associated with the Service Portal Transition.

Design Customizations. The Portal configuration process shall be an Agile-style iterative process providing rapid feedback throughout. At the start of the project, Contractor shall collaborate with the County in several iterative workshops to design the Portal "look and feel" and to review initial functionality. The configuration process that takes place during the Transition period shall include items such as the following:

- County branding and "look-and-feel" elements on the front page (tiles, menus, links)
- Use of banners and splash pages
- Identification of End-User roles to be configured, to determine which groups have access to the various types of information
- Integration with Active Directory for Single Sign-on and configuration of End-User roles
- Integration with Service Manager and other tools
- How existing portals and data sources (ITSC, Doc Vault, and so forth) shall be presented—as links or tiles from the main page to the existing functioning applications.

Service Portal Implementation. During transition, Portal implementation has two parts: (1) the "look and feel" of the Portal and (2) integrating HPE Service Manager (SM) and other applications and data sources. Contractor shall begin with a sample portal and gather feedback from the County to determine the County's preferences. This shall be an iterative process, and once finalized and approved by the County, it shall become the Transition release design version.

With Portal design in hand, the next task shall be to connect the functionality of the document repositories and portal systems in use today to the appropriate tiles or links in the new Portal design. The integration of Service Manager with the Service Portal shall be part of Contractor's product integration. The functionality in the Portal that is embedded in Service Manager shall require minimal configuration. For Transition, there shall be no change in the application functionality of existing source applications that sit behind the Portal (those reached by pass-through links and that are not part of the Service Manager suite).

Testing. With the design complete and built, the Portal and attached functionality shall be tested. Contractor shall use the testing methods used for other infrastructure and applications releases, progressing from Systems Integration Test (SIT) through User Acceptance Test (UAT).

Content Development, Content Migration, and Training. In the same timeframe as the testing phases, Contractor shall create Service Desk related content, such as self-help content (videos, tip sheets, and so forth) and cross-functional content associated with the Service Desk available on the Portal. Contractor shall create Service Desk scripts and conduct training for the Service Desk agents to support the Service Portal, and work with the County to develop training and communications materials to introduce users to the new capabilities.

At the end of the process, Contractor shall present final documentation and the Portal itself for County review and response. Approval and successful completion of the activities above shall mark the end of the Service Desk Framework Transition. During the rest of the framework transitions, reports, updated process documentation, design documents, and other deliverables shall be posted to the Service Portal as these deliverables are completed.

- Automated systems and tools involved in solution

The Service Portal shall be customized using End-User Access (EUA) and other web development tools.

Contractor shall use Project and Portfolio Management Center (PPMC) as Contractor's Primary Project and Portfolio Management (PPM) tool suite. Contractor use PPMC for the development and ongoing management of project schedules.

9. TRANSFORMATION PROJECTS

9.1. Transformation Services

Contractor shall control transformational projects through Enterprise Architecture (EA) governance processes that incorporate CTO architecture principles, bricks, reference patterns, technology assessments, regular meetings and roadmaps to identify and align solutions suitable with County business and IT strategic direction. Contractor's CTA and Contractor's EA team shall continue to lead innovation days and technology seminars, focusing on improvements to keep the County moving forward. Contractor shall establish actionable roadmaps with measurable objectives to forecast and accommodate business changes in an agile orientation through effective governance and processes that:

- Use EA tools such as MEGA to create artifacts to identify, allocate, and measure transformational initiatives from an end-to-end perspective
- Establish a Transformational Maturity Model (TxMM) and analytical algorithms to analyze, predict, and recommend architectural and transformational initiatives
- Establish a Model Driven Enterprise in which service models are used to simulate and test emerging value chains and alternatives and accomplish prototyping and testing without impacting operational baselines
- Incorporate recommendations based on bi-modal organizational thinking.
- Blend bi-modal approaches to build County services from an "Outside-In" perspective.

Contractor shall leverage Contractor's knowledge of the County environment, business processes, and strategic objectives.

- Solution Summary and Rationale

The following section sets forth Contractor's approach to addressing the individual Transformation Projects, as listed in the table below. These projects shall be undertaken at the County's request, follow standard Service Request procedures, and shall include no less than what is described in this Transformation section.

Transformation Projects

TRANSFORMATION PROJECTS
Desktop Services
User Data Services
IT Application Portfolio Management Services
Network Transformation
Voice Services Transformation
Storage Architecture
E911
Identity Federated Services
Enterprise Information Management (EIM)
Comprehensive Applications Threat Analysis (CATA) Service

Desktop Services Transformation Project

- Solution Summary & Rationale – Description of solution to meet the requirements

At County's election, Contractor shall implement Presentation Virtualization (also known as Application Virtualization) driven by Citrix XenApp. Presentation Virtualization helps address the need by decoupling the legacy applications from the device in such a way that it minimizes the infrastructure and overall costs when compared to other virtualization approaches. In doing this, legacy applications no longer dictate the upgrade path for the rest of the County's environment and this minimizes the potential for impact if a particular application such as Kronos, Acclaim, or Accela causes problems with the latest O/S upgrade, or browser version. This, and all of the other virtualized apps, can remain for as long as the County continues to use the apps. Transformation of legacy apps can then proceed on their own timeline, rather than being tied to the remainder of the IT environment.

Each virtualization option, illustrated in the Compute Style section of the figure below, is generally related to a specific type of End-User's digital profile, and is typically based on their overall work related IT requirements (e.g. Device(s), Applications, Data, and Support). As the need for more computing power increases (i.e. CPU, Memory, graphics) at the End-User level, the more complex and costly the virtualization solution becomes.

Project Deliverables:

- Virtualization of up to 200 County applications
  - For up to 15,000 County Users

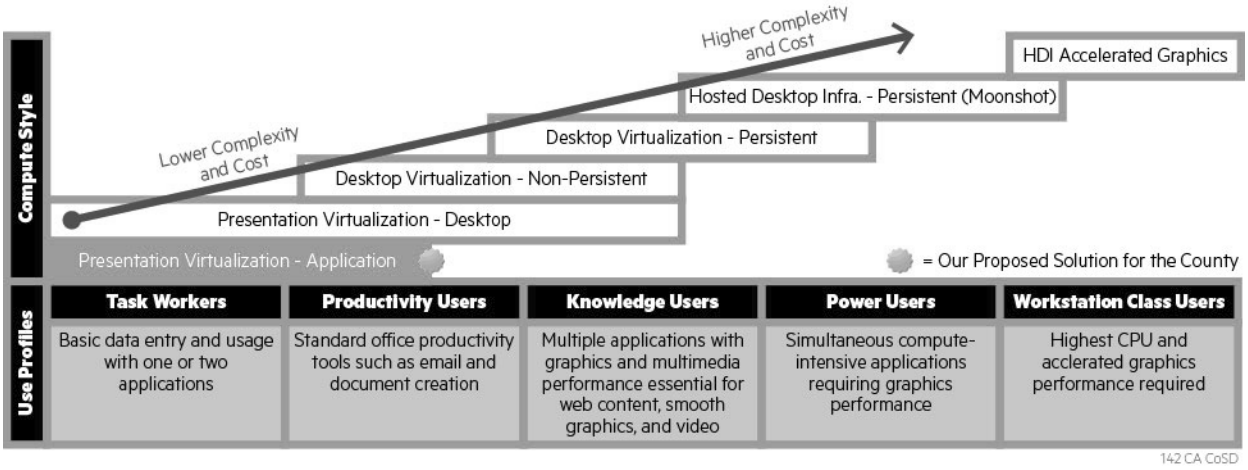
Contractor assumes High Concurrency of End-Users, meaning that for the most part, multiple users would be accessing the application(s) at the same time.

Client virtualization processing load is not only determined by the number of concurrent users, but by the complexity of their applications. The greater the application complexity, the lower the End-User density per server. As a result, application complexity is an important determinant of the number of concurrent users that can be supported on a given Client Virtualization Service (CVS) solution. Contractor classifies application complexity into three groups: light, medium, and complex and has assumed an application profile of medium complexity for the County. Medium Complexity is a standalone application that has minor dependencies on the OS, a prerequisite application, or large/complex data feeds. Most business-related common off-the-shelf applications are considered medium complexity. One notable exception is Microsoft Excel workbooks with embedded macros that can be considered complex in nature.

Specific deliverables include:

- CVS design assessment
- Detailed Presentation Virtualization solution design
- Implementation of the approved solution
- Standardized Contractor CVS Presentation Virtualization monthly reports.

Presentation Virtualization



The approach decouples the legacy applications from the device in a way which minimizes the infrastructure and overall costs compared to other virtualization approaches.

Rationale: Presentation Virtualization, provides all the required functionality and is significantly more cost-effective than other solutions, such as VDI (i.e. Desktop Virtualization, both non-persistent and persistent). Contractor recommends a periodic re-evaluation of Client Virtualization after a number of years, perhaps making the next step to VDI if the requirements change, and if it makes sense financially for the County. This would also be a time to review the current desktop build from the ground up, since VDI would require a much thinner client.

Contractor designed the solution for the County to use the same software stack and versions to deploy and to manage it throughout the life of the Agreement. The solution includes:

- Lakeside Software's SysTrack (for Assessment)
- Citrix: XenApp, XenServer, NetScaler
- Microsoft Server, SQL
- AppSense DesktopNOW Environment Manager.
- Liquidware Labs 'Stratusphere™ UX', Profile Unity and FlexApp
- HPE's Standard Reference Architecture
- Automated Tools – Automated systems and tools involved in solution

Contractor's analysis shows that typically 80 to 90 percent of the use cases can be met by presentation virtualization (typically Citrix XenApp). Presentation virtualization is the most cost effective way to deliver legacy applications when compared to other desktop virtualization technologies, including VMware solutions.

Desktop product upgrades or changes to the Applications Portfolio require significant time and engineering efforts to deploy. Presentation virtualization addresses this issue in that upgrade engineering and testing need only focus on one image: that of the server in the data center running the application that is being presented to the End-User. Virtualizing desktop applications removes a dependency on various desktop client hardware.

This helps prevent deployment delays and post-deployment problems while improving the ability to rapidly maintain desktop currency, at least for the many desktop applications that are virtualized.

Presentation virtualization shall also help maximize the performance of all the applications on the End-User device, whether virtualized or local.

Timing: The Presentation Virtualization project would follow Transition completion.

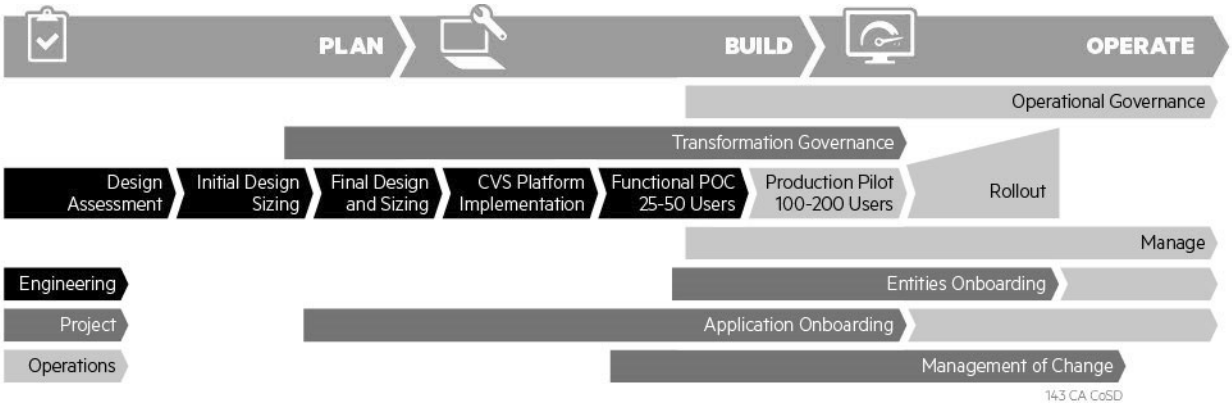
Risk Considerations: The introduction of client virtualization changes the way users perform their work and is therefore considered disruptive. Failed first attempts to introduce users to client virtualization result in roll-out delays, onboarding program rework and reintroduction to users which is costly, time consuming and can significantly erode the expected ROI. For a high degree of success, consider the following:

- **Entity onboarding** - Depending on the structure of the customer and according to the priorities defined during the assessment/analysis/design phase, Contractor recommends ramping up users by personas (groups of users). End-User personas could be a business unit, a department, a typical group of End-User profiles based on common desktop or application requirements. This involves identifying people, managing the persona grouping, desktop and application group entitlements and orchestrating this by means of Active Directory.
- **User onboarding** - Onboarding management and Client Virtualization Service (CVS) Management links the two onboarding subphases (Entity and User onboarding). Contractor proposes to migrate a category of virtualized users either by a specific persona and/or with relatively similar desktop/application requirements, and begin with less complex use cases then progress to the more complex. Subsequently, the scope will be increased until all users have been on-boarded successfully.

All onboarding activities are managed and controlled by an onboarding manager. Once users are successfully onboard in the production environment, they are managed like any other End-User with a CVS Service Manager. The CVS Service Manager monitors the overall performance of the virtualization service, coordinating performance review meetings and reports with both the customer and CVS operations.

Key dependencies and Milestones: Contractor's proposed deployment is comprised of two discrete parts, with the second part dependent upon completion of the first. These are CVS design assessment and implementation.

Representative Key Milestones for a Presentation Virtualization Deployment



Durations and dates of the major tasks are dependent upon the data gathered from the first step, the Design Assessment. After the Design Assessment, Contractor develops the final implementation timeline. Typical Presentation Virtualization projects of similar complexity to the County's take approximately five months.

- Deployment plan for resources and use of facilities

The following Contractor resources shall support this transformation project:

- The Contractor Workplace Transformation Consulting Team shall perform the CV Assessment
- The Contractor implementation team consists of
  - An overall Program Lead that is a subject matter expert (SME) in End-User Compute solutions.
  - Additional SMEs based on the overall solution scope and may include but is not limited to: project management, deployment and implementation planning, infrastructure specialists, End-User onboarding, training, Image Creation / Mgmt., application packaging and testing.

- A senior Transformation Manager who is responsible for the end-to-end project scope and stays in place until acceptance criteria have been met.
- Ongoing support for the Presentation Virtualization service shall be delivered by US-based delivery resources in line with the County's requirements.

- Methodology & Key Processes – Key methodologies and processes in solution

Contractor follows a proven methodology for CVS implementation that begins with the CVS Design Assessment, and continues through implementation and ongoing management as described below.

CVS Design Assessment: Contractor shall assess a sample of existing County users, looking at how they interact with their apps and analyze how the apps interact with users' devices. This helps the appropriate applications for each End-User type to be identified and drive the transition plan from the current mode of operation (CMO) to the desired future mode of operation (FMO). This assessment would take into consideration the following items:

- The desktops included would be a sample of End-User desktops for each type of user and IT usage
- A "Type of End-User" categorization, which refers to the type of applications users work with the intensity with which they use them as measured by CPU, RAM, disk IO, and network traffic
- A "Type of usage" categorization, which includes not only the PC, laptop, tablet, smartphone, or engineering workstation each End-User needs to do his/her job, but also any requirements for peripherals such as USB connected security dongles, portable data storage, cameras, meters, and other specialized devices. The goal is to identify the subset of IT usage that provides the majority of business value, identify a solution that meets the core requirements for providing that business value, and, after the core requirements are met, identify how to support all other candidates for virtualization for the optimum incremental cost.

There are three steps to the Design Assessment:

- Startup
  - Developing a statement of requirements to confirm that the engagement team understands the purpose of this engagement from the County's point-of-view
  - Developing a data collection plan that details how the engagement would collect the data needed for this assessment: The purpose of this plan is to enable County personnel responsible for change management and information security to approve the data collection.
- Execution
  - Meeting notes from a discussion of the County's intended future mode of operation (FMO) to confirm that engagement team understands the desired outcome
  - An assessment report that summarizes and analyzes the collected data: The engagement team would review this assessment with County stakeholders
- Closedown
  - A solution document that identifies the next steps that the County and engagement team have jointly recommended as a result of reviewing the assessment report.

This assessment validates the initial assumptions or identifies necessary modifications of the initial assumptions related to the original scope for this effort. This revised scope, based on the data that was gathered and analyzed, can affect the original solution and can have an impact on the overall solution components including; infrastructure, labor and software that is required for the solution.

CVS Implementation: At the start of the implementation phase of the project, Contractor holds a workshop to begin the planning process. Contractor would work collaboratively with the County to identify and agree upon key milestones and objectives, and Contractor would report status on these throughout the implementation.

Contractor has an established and proven transformation methodology that follows an industrialized "factory" approach. This methodology is organized in phases, as described in the following overview, with clear milestones

that are established by Contractor and the County after the Design Assessment. Contractor then creates a mutually agreed to transition plan with a detailed work breakdown structure, milestones and owners for execution.

The activities executed during the Implementation Phase of the project are:

- Design Sizing (Initial, Final)
  - Review of assessment data (End-User usage, application usage, network, End-User data, security)
  - Architecture Design and Infrastructure Implementation Plan established
- Infrastructure Set-up
  - Site preparation in the Tulsa data center and equipment provisioning. This environment can be implemented as an expansion to the County's MPC environment, or as a standalone virtual infrastructure under the HMCB, in order to integrate it with the County's hybrid cloud.
  - Server installation (HW and operating system)
  - Server integration in the County's Active Directory Domain
  - Server integration in the Tulsa data center and linkage to other infrastructure service (DNS, Storage, proxy, AV system, etc.)
  - Software implementation and configuration
- Functional Testing
  - Functional pilot or Proof of Concept (POC), is performed by a small group of IT users to verify compliance (to functional and technical requirements) and performance of the solution, and tune the configuration if necessary.
- Production Pilot
  - While the functional testing above is focused on IT users with client virtualization familiarity, this testing phase focuses on the general End-User population with the goal of testing both the technical solution and the roll-out plans and materials.
  - The Production pilot is performed with 100 to 200 selected users operating in the production environment. This pilot is for a fixed, short period of time. Test scripts are supplied to pilot users that identify the specific activities a participant is to perform. Contractor then examines the results for faults and provide feedback to the delivery team. Contractor corrects any faults, either by correcting the script, End-User performance of the script or infrastructure/software correction. Once corrections are in place, Contractor would re-run the script until all test scripts are successfully completed with no issues.
- Onboarding
  - During this phase, Contractor manages two kinds of onboarding (Entity and User, as mentioned above), each of which potentially influence the other. Workgroup/departmental similarity in application use, security, and the County's implementation priorities are the main factors in identifying a roll-out plan.
- Management of Change
  - Throughout the entire pilot and rollout period, the Transformation Manager would work with the implementation team and the operational support team to verify that the rollout plans are communicated, support is in place and End-User issues are addressed.

User Data Services Transformation Project

- Key Considerations and Potential Alternative Approaches

One of the steps to achieving a truly mobile workforce is to separate the data from the device. By doing so, County employees would be able to access the data necessary for their job from any number of devices, whether County-owned or through Bring Your Own Device (BYOD), or even via the Web. Knowing this, Contractor has formulated a number of key considerations. The solution must have the following characteristics:

- Be secure
- Allow End-User data to be decoupled from the End-User's device
- Take advantage of existing licensed solutions, tools, and services
- Allow various levels of access.

- Support collaboration both within the organization and external to it.
- Finally, County users span many different types of work, and they are multi-generational as well. Because of this, Contractor's solution balances a new way of interacting with one's data along with the need to maintain some form of familiarity.

- Description of solution

Contractor recommends taking full advantage of the technology the County already has using the County's Office 365 subscription and OneDrive for Business.

OneDrive for Business includes apps for smartphones, and allows mobile access through the mobile device management (MDM) solution.

As subscribers to the G3 level of Office 365, each End-User has 1TB of space on their OneDrive for Business account. Microsoft research shows that the vast majority of business users consume much less than 1TB Contractor's research on the County's historical use of file shares supports this. The entire size of County network shares is 78TB for all 15,000 users. Contractor would continue to work with Microsoft to facilitate optimal configurations.

End-Users can collaborate in several ways. Using OneDrive for Business, an End-User can share a document or series of documents from their own OneDrive for Business data space. The documents themselves are not delivered to the other End-User. Rather, a link to that document allows the designated End-User (and no one else, besides the owner) access to only the documents the owner wants to share.

Departments or divisions that want to have a shared space for their exclusive use can create "groups." Access to these groups is initially fully locked down. The owner of the group would have to explicitly invite members to use the shared space.

To fully realize the benefits of Office 365, users must make the move from using network file shares to storing their data on OneDrive for Business. Contractor proposes a project to migrate data on End-User network file shares to their OneDrive for Business location. The project steps at a high-level are:

- **Group Policies / Powershell Scripting.** The moves would be automated via Powershell scripts and actioned via group policies.
- **Search for invalid files/folders and cleanup.** OneDrive for Business has different requirements for filenames and folder structures than Windows. Contractor would need to locate the files that would not move in their original states.
- **Pilot.** Contractor would migrate a test group of users via automated processes.
- **Scheduling.** The migration would need to occur in waves. The project plan assumes a conservatively low size of 300 users per wave. As the waves progress, the size of subsequent waves might grow, thereby shortening the project.
- **Communication / Training.** OneDrive for Business is a paradigm shift from the traditional way of interacting with data files. Contractor would develop and deliver a communication plan as well as training for users who migrate to OneDrive.
- **Migration (waves).** The migration would occur in waves, with support throughout the entire project. At the end of the project, all County users would have completed a migration from a network share data to their OneDrive for Business account.

- Deployment plan for resources and use of facilities

For OneDrive for Business, all data is stored in Microsoft's Government Community Cloud.

Support for OneDrive for Business would come from the Service Desk. OneDrive for Business issues would take advantage of Contractor's enhanced support for Office 365 service, which uses Contractor support resources working on-site with Microsoft Office 365 support engineers.

- Methodology & Key Processes – Key methodologies and processes in solution

Contractor supports OneDrive for Business, using time-tested infrastructure processes of both HPE and Microsoft, which emphasize delivering measurable, repeatable, and efficient services to the End-User.

- Automated Tools – Automated systems and tools involved in solution

For the rollout and subsequent maintenance of the End-User device connectivity to OneDrive for Business, Contractor would use Group Policy through Microsoft System Center Configuration Manager (SCCM). This would allow a smooth rollout of the solution and would make subsequent revisions for new requirements easier as well.

- Qualifications and Experience – Background and experience in comparable environments

Internally, Contractor has transitioned ~300,000 users (HPE/HPI combined) to OneDrive for Business, using it for individual storage, collaboration, sharing, and device backup. Contractor would follow a similar process to successfully migrate the County to the OneDrive for Business solution.

This solution takes advantage of Contractor's 30-year history of partnership and collaboration where Contractor is the only Microsoft partner to have co-located shared support resources for Office 365 for the exclusive use of Contractor's customers.

IT Application Portfolio Management Services Transformation Project

- Key Considerations and Potential Alternative Approaches
-

IT Application Portfolio Management supports the continuous assessment of IT application portfolios to:

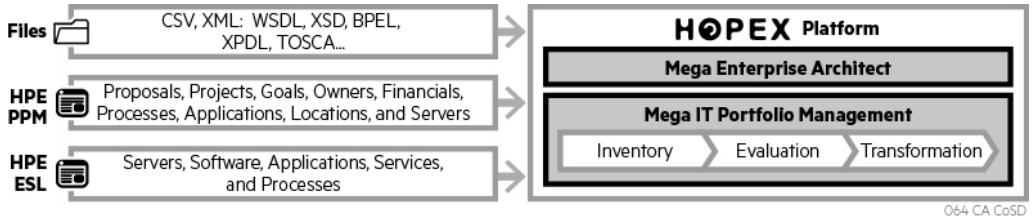
- Standardize portfolio management
- Align the IT application portfolio with business strategies
- Reduce deployment time
- Improve operational efficiencies
- Reduce costs and optimize value
- Increase visibility and understanding of the application portfolio

Key considerations for this transformation project require selecting a tool suitable for meeting the criteria listed below.

- Highly configurable
- Integrated environment
- Integration with source systems
- Speed of implementation
- Develop architecture disciplines to maximize in-place tools
- Business capability mapping
- Incorporation of application portfolio inventory
- Define cost elements
- Project-related information
- Rationalization alternatives/recommendations

- Solution Summary & Rationale – Description of solution to meet the requirements **Solution:** MEGA's HOPEX platform offers a comprehensive, well-rounded, feature-rich platform that provides an out-of-the-box metamodel that is highly configurable and has strong modeling capabilities. It also supports a wide range of industry frameworks. HOPEX combines industry-leading practices in enterprise architecture (EA), IT portfolio management (ITPM), business process analysis (BPA), and governance, risk, and compliance (GRC) into a single platform. This integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation as shown in the figure below.

MEGA IT Portfolio Management



This fully integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation.

Use of this tool facilitates creation of a complete inventory of IT assets, including applications, underlying technologies, and servers. Both out-of-the-box and custom reports provide information that makes it easy to evaluate IT assets using multi-criteria analysis such as costs, risks, technical efficiency, and business value, bringing visibility to the County's IT portfolio. This information also provides insight about dependencies and helps to identify redundancies of IT systems while reducing costs and complexity by eliminating systems with the same functionality. MEGA also provides the ability to create and compare multiple transformation scenarios that take into account various criteria to select the most relevant scenario for their business needs and constraints.

Upon approval from the County to proceed with this transformation project, Contractor and MEGA consultants would schedule a project planning and kickoff meeting. A topic of discussion for this meeting would be identification of County stakeholders that requested to participate in requirements gathering sessions to make certain the MEGA ITPM is configured correctly to meet the requirements.

Once in place, MEGA ITPM provides a three-step approach to managing IT assets:

1. **Inventory**: ITPM automates the collection of IT assets through a web-based interface. It provides metadata that can describe IT assets through various parameters such as functional scope, lifecycle, costs, and risks, providing a comprehensive view of the existing IT portfolio.

The inventory creation would use MEGA's APIs to interface with the ESL, partner systems, and other feeder systems (i.e., AppsManager) to make certain accurate data is in place. Once the inventory data is populated, IT assets can be viewed by business lines, business processes, business capabilities, organizational units, and technology vendors.

2. **Evaluation**: This step assesses IT assets through either out-of-the-box or custom criteria such as costs, risks, business value, and functional support. It provides detailed analysis through cost, dependency, and impact reports (i.e., brick's compliance). To rationalize the portfolio, it provides insight into which IT assets need to be removed, replaced, or maintained. Using business capability maps, IT assets are organized by functional areas, and changes are displayed over time, helping to make better-informed decisions.

Also during this step, costs and other project-related information are associated with the assets. The IT assets are evaluated by business value, functional support, and technical efficiency through the use of IT portfolio evaluation campaigns.

3. **Transformation**: In this step, the County can define a mix of initiatives or assumptions such as extending, replacing, or phasing out applications and technologies and compile them into different scenarios. The County can then assess and compare these scenarios through various criteria such as risk to quality, risk to feasibility, and costs and then identify the best transformation scenario to implement.

Rationale: Contractor has designed this project based on the recommendations of the MEGA ITPM tool product supplier, with the following characteristics and caveats:

- As requirements evolve, additional MEGA modules, such as Enterprise Architecture and Governance, may be required.
- Information from the Contractor's ESL, PPM, and AppsManager would be maintained by the source systems and would be updated by MEGA at scheduled times.
- MEGA out-of-the box functionality would be used for this effort.
- Contractor would install, configure, and manage MEGA modules.
- Licenses are included for MEGA HOPEX WorkBench and ITPM module for 30 contributors, 10 Portfolio Managers (GITMs) and 5 Advanced Users (CTO).

Timing: Contractor proposes to use the MEGA Quick Start program for implementation of MEGA ITPM. In the MEGA Quick Start program, Contractor would collaborate with MEGA consultants to conduct a project kickoff that includes the definition of project scope and schedule. Typical installation and configuration of a MEGA project takes about 45 days, including installing and configuring MEGA ITPM, conducting functional/deployment specifications workshops, designing supporting MEGA metamodels, testing the changes, reviewing and mapping the artifacts, uploading the artifacts, establishing portfolios and hierarchies, and training supervisors and users.

Risk considerations: Potential risks that could affect the project include the following:

- Automating APIs and metamodels shall require configuration and potential connector development to accommodate integration with external systems of record: AppsManager, PPM, and HPE's ESL.

Key Dependencies and Milestones: Following are the key milestones and dependencies for the project:

- Kickoff: Receipt of County approval to begin would initiate kickoff of the engagement. After the kickoff session, Contractor would define the project scope and develop the schedule.
- Installation: The next milestone is installation of MEGA on the established infrastructure. This is dependent on the availability of SQL Server licenses and availability of the infrastructure.
- Specification: The next milestone is conducting and delivering the functional/deployment specifications workshop. Part of this deliverable would be demonstration of MEGA ITPM capabilities. Contractor would prepare an ITPM customer guide. The deliverable would include the functional/deployment specifications and customer guide. This task is dependent on availability of the designated County users who would provide the requirements for use of the MEGA system.
- Configuration: The next milestone is reached when the configuration and customization of MEGA is completed using the functional/deployment specification as defined above. During this step, the supporting MEGA metamodels would be designed, built, tested, and implemented.
- Artifacts: The next milestone is reached when all artifacts are uploaded in MEGA after reviewing and mapping the ITPM specific artifacts. The portfolios and hierarchies would also be established during this cycle. At this time Contractor performs acceptance testing to verify that it is set up correctly.

- Training: This milestone would be followed by a training session for users.

- Deployment plan for resources and use of facilities

Resources: For implementation of the MEGA ITPM toolset, Contractor would use MEGA's Quick Start program. MEGA's experienced consultants would work with Contractor to install, configure, and set up the MEGA environment. MEGA consultants and Contractor staff would work with County staff to demonstrate MEGA HOPEX functionality, determine functional and deployment needs, and document the supporting requirements. To minimize the County's time investment while maximizing impact, Contractor would conduct information gathering workshops through a series of focused discussions with stakeholders to make certain that Contractor has an accurate understanding of the County's needs. At the end of this effort, Contractor would deliver a functional deployment specification and an End-User guide. Contractor would then help design MEGA metamodels and make the configuration changes to interface with PPM, ESL and AppsManager systems. Contractor would then upload the artifacts and establish portfolios and hierarchies in accordance with the County's needs. Contractor's team would also provide training for the End-User groups who would use MEGA ITPM toolset.

The Contractor team supporting the MEGA toolset would work closely with CTO, and supporting staff to provide a collaborative working environment. This would enable direct communication and provide the County with the ability to reach out directly to Contractor personnel for quick resolution of any issues.

Facility: Contractor would locate the MEGA infrastructure in the Tulsa data center.

- Key methodologies and processes in solution

Contractor would perform the installation, configuration, and management of the MEGA ITPM toolset using ITIL v3 processes, consistent with the established processes for managing County assets. Contractor would use Contractor's system development life cycle (SDLC) processes in collaboration with the County staff to configure and make necessary updates to MEGA application programming interfaces (APIs) to align with automated systems and tools involved in Contractor's solution.

The MEGA ITPM tool provides all required functionality to meet the County's requirements, and it would integrate with AppsManager, PPM and the ESL solution.

Network Transformation Project

- Description of solution to meet the requirements

The Contractor's approach to network transformation leverages the existing investment that the County has made in its infrastructure, building on the robust, geo-redundant network core to enable new service adoption while Contractor migrates from legacy technology. This foundation positions the County to make smart, progressive choices in the way services are delivered to its employees and constituents, regardless of their location or access device. As the County network continues to evolve, Contractor's ability to provide ubiquitous connectivity with seamless accessibility, security, and performance would provide the benchmark of Contractor's framework.

Cloud Enablement via NetBond

As cloud-based services mature and become more viable for Government use, Contractor is positioning the County's network perimeter to enable seamless, secure, and performance-assured integration for cloud providers. Contractor shall cause AT&T to build a geo-redundant core network foundation to enable this shift in services, leveraging AT&T's virtual private network (AVPN) MPLS-based transport. This foundation is to be deployed as a Transformation activity in preparation for future services.

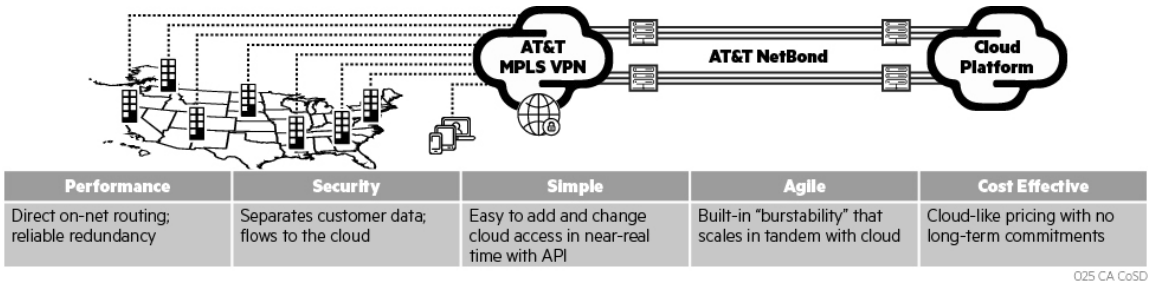
Building on Contractor's AVPN transport, AT&T's optional NetBond service would be made available on a per cloud provider basis, enabling secure, performance-assured cloud-to-enterprise peering, in turn isolating these

important services away from the unsecure and potentially congestion-prone Internet Service Provider (ISP) links. The NetBond service is represented as a proposed new RU, where the County can select peering relationships with designated cloud providers on a bandwidth scaling basis. Cloud provider side costs may apply and would be priced as new RUs when establishing a new cloud provider contract, as requested by the County.

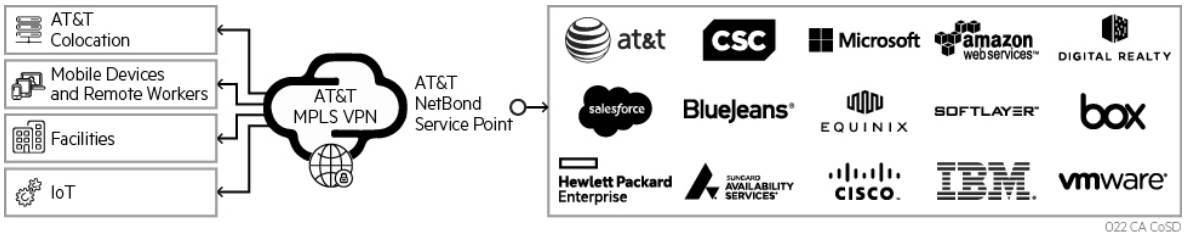
AT&T's NetBond service would terminate at the County's edge, providing a geo-redundant presence in line with stated objectives; coupled with the inherent redundancy of the Global AT&T Multiprotocol Label Switching (MPLS) infrastructure, NetBond would provide the highest available level of resiliency, to enable the continuity of the County presence and its ability to conduct business.

In support of the transition of Exchange to the O365 cloud, AT&T would enable Netbond functionality in a peering arrangement with Microsoft's ExpressRoute product. This would be designed and implemented in line with the specified transition plan and is priced as a separate resource unit that combines the NetBond RU with the ExpressRoute costs to complete the connectivity model for the service.

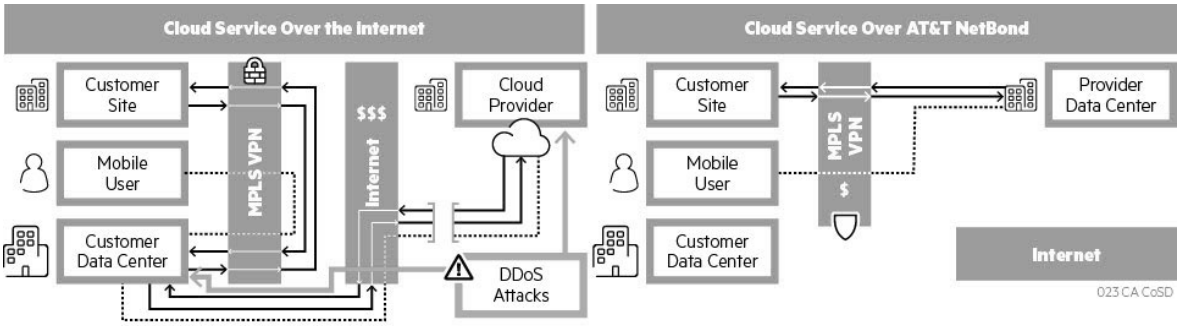
AT&T NetBond Benefits



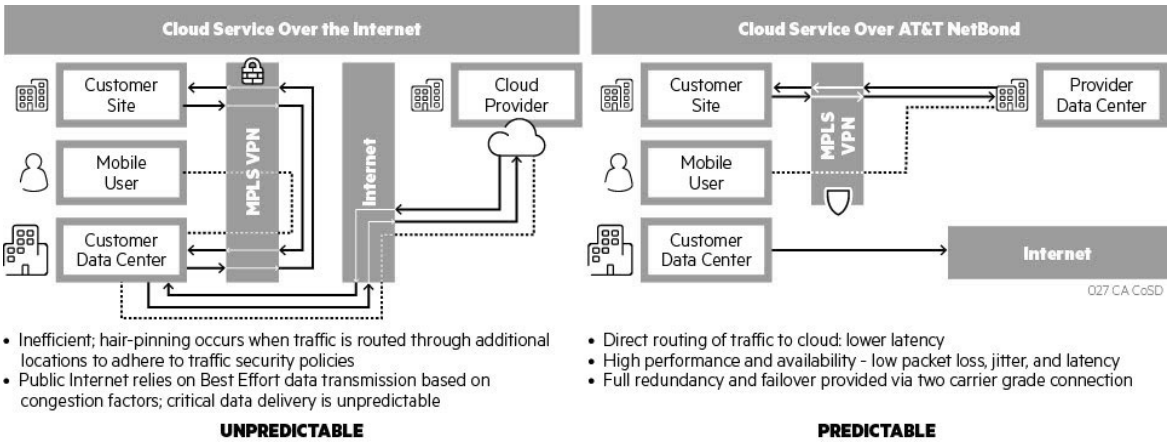
Well-known cloud services partners that AT&T currently supports via NetBond.



Security Benefits of AT&T NetBond



Performance Benefits of AT&T NetBond

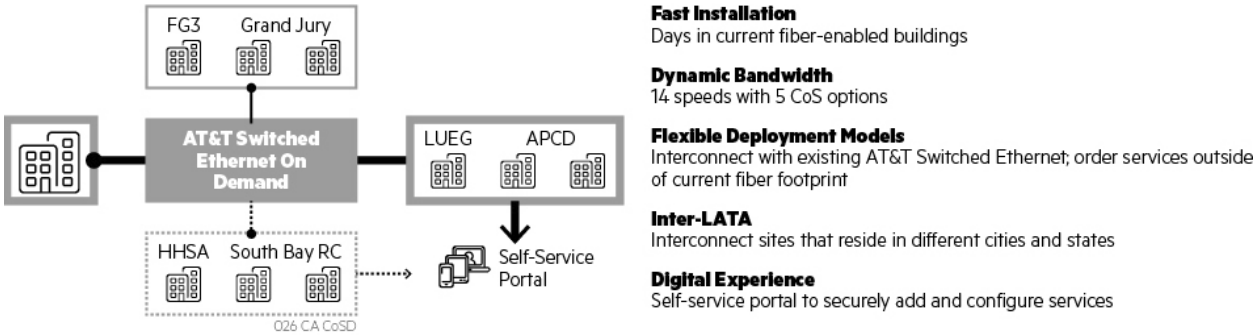


Migration to AT&T Switched Ethernet with Network on Demand

Contractor's transformation plan for the County's wide area network (WAN) includes migration of all 115 OPT-E-MAN Metro Ethernet connected sites to the AT&T Switched Ethernet with Network on Demand (ASE w/NOD). Additionally, all data T1 sites shall be evaluated for migration and where available without significant special construction costs, sites shall be migrated to this new service. Special construction costs apply when fiber based transport is unavailable in the "last mile" from an underground or above ground exchange nearby a given site. The fiber install from these local exchanges is included in normal construction, but installing extended runs to new areas with no local exchange would be grounds for special construction. During the design and provisioning process, Contractor shall provide a list of T1 sites to the County with special construction costs for consideration. It is believed that 80-90% of the existing T1 sites are eligible for migration to this new service.

Using software defined networking (SDN) capabilities inherent to ASE w/NOD, bandwidth can be adjusted within 15 minutes from as low as 2 MB to as high as 1 GB. Coupled with real-time capacity management capabilities, this new service would allow rapid response to County bandwidth needs as well as enable the planning of additional throughput for scheduled events. Additionally, the deployment of fiber-based services would further improve consistency, availability, and performance of the remote sites across the network. The figure below lists benefits of AT&T Switched Ethernet On-Demand Service.

Figure 3. AT&T Switched Ethernet On-Demand Service Benefits



ASE w/ NoD Site Redundancy

Contractor has evaluated enabling additional remote site redundancy at key County facilities. The facilities listed below are historically some of the most important to County business functions and are the recommended sites for this enhanced service. It's important to note that the site list includes two sites that are currently on the Gigabit backbone (Sites 18 & 33), but are planned for migration to ASE w/ Network on Demand as a part of the Network Transformation, Backbone Consolidation project (see next section).

Site #	Site Name	Street Address	City	Zip Code
13	Children's Service Center (Adoptions Center)	6950 Levant St.	San Diego	92111
18	MTS Trolley Tower (Mills Building)	1255 Imperial Ave.	San Diego	92113
19	Lemon Grove District Office / FRC	7065 Broadway	Lemon Grove	91945
33	Health Services Complex	3851 Rosecrans St.	San Diego	92110
35	Animal Control-Central Shelter	5480 Gaines St.	San Diego	92110
55	Oceanside Service Center	1315 Union Plaza Ct.	Oceanside	92054
56	A. B & Jessie Polinsky Children's Center	9400 Ruffin Ct.	San Diego	92123
57	Child Welfare Services - Central	4990 Viewridge Ave.	San Diego	92123
80	Assessor/Recorder/Clerk Kearny Mesa	9225 Clairemont Mesa Blvd.	San Diego	92123
81	Assessor/Recorder/Clerk San Marcos	141 E. Carmel St., Bldg. 1	San Marcos	92078
95	HHSA FRC Center South Bay	401 Mile of Cars	National City	91950
190	HHSA FRC Center Escondido	649 W. Mission Ave.	Escondido	92025
205	Edgemoor Geriatric Hospital	655 Park Center Dr.	Santee	92071
260	Assessor's Revenue and Recovery	590 3rd Ave.	Chula Vista	91910
290	Access 211	8765 Fletcher Pkwy.	La Mesa	91942

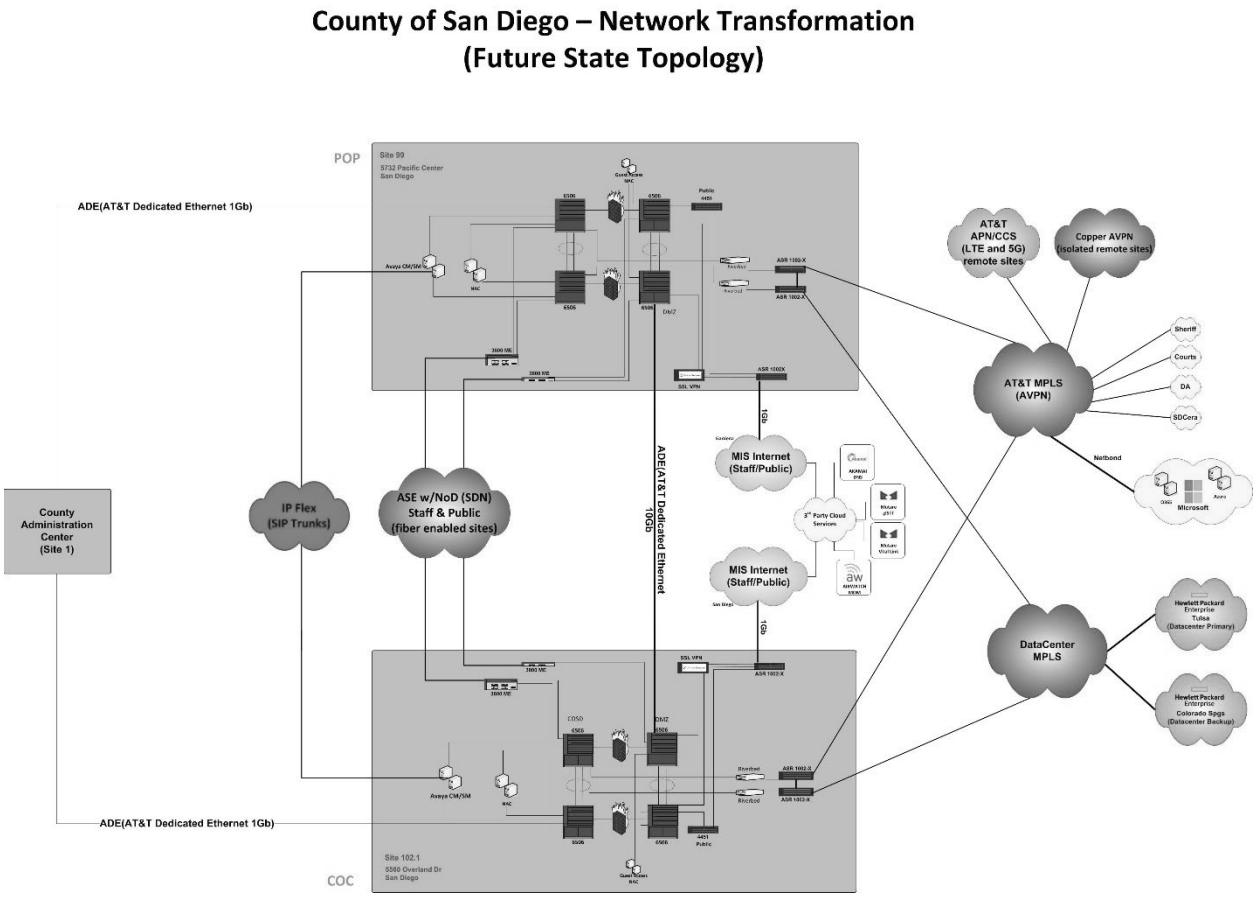
The standard Network on Demand design provides geo-redundant host circuits, however from the last Central Office, this diversity is reduced to a single fiber pathway to the remote site. The redundancy design involves provisioning a redundant circuit with diverse fiber path and infrastructure from an alternate central office. This secondary pathway extends to the remote site, entering via redundant entrance facilities. The circuits shall be ordered and built as stand-alone circuits and configured with minimal bandwidth, which leverages the Network on Demand near real time bandwidth provisioning capability to provide fully functional bandwidth in the event of a failure on the primary path.

Contractor shall provide the completion of requisite core transport design work which shall result in a per site construction cost for County consideration. This process shall also allow the County to evaluate cost of diverse entrance facilities. These one-time costs are responsibility of the County. The County may evaluate these costs and select sites that have the greatest benefit without being cost prohibitive. As these sites are selected, and one-time costs agreed, Contractor shall execute an order for the service. This offer shall remain valid over the first four (4) years of the contract term. County requests to add sites not previously listed shall be handled on a case by case basis.

Backbone Consolidation

AT&T also adheres to the concept of keeping it simple where possible. While some network solutions can be incredibly complex, the core architecture does not have to be. By reducing the number of core backbone sites (GigaMAN Connected), AT&T can simplify the network architecture while providing redundancy, sufficient bandwidth, and throughput for County business. This allows Contractor to right-size and tailor services in accordance with the needs of a location without the costs, equipment, and infrastructure inefficiencies that come with unnecessary capacity. The net result is standardization of transport connectivity across all County sites, providing the shortest path to services, in turn leading to predictable performance, improved security, reduced maintenance cost, and lower mean time to recovery (MTTR) in the event of an incident. The figure below illustrates the future-state network topology.

County of San Diego Network Transformation (Future State Topology)



Session Initiation Protocol (SIP) Core Expansion

Contractor's network team has already begun the process of transformation within the County to phase out Time Division Multiplexing (TDMbased voice connectivity in favor of Session Initiation Protocol (SIP)-based solutions. Contractor's SIP infrastructure is provided via two geo-redundant AT&T IP flex trunks that are dynamically available and sized to take a full production load of traffic in the event of a circuit failure. Currently, the SIP trunks are configured to support local outbound calling. Expanding on this foundation, Contractor plan to increase the capacity of these trunks to enable support of all Avaya core network controlled outbound calls, including local, long distance, and toll services. This expansion would eliminate outbound usage-based costs for these legacy resources units. Inbound calls would be migrated to SIP including Toll Free 800 services, which would substantially reduce the usage charges associated with Toll Free 800 services. Over the life of the Agreement, Contractor would continually evaluate the capabilities of these trunks to support additional voice and unified communication services.

Future T1 Migration for Non-ASE with Network on Demand Sites

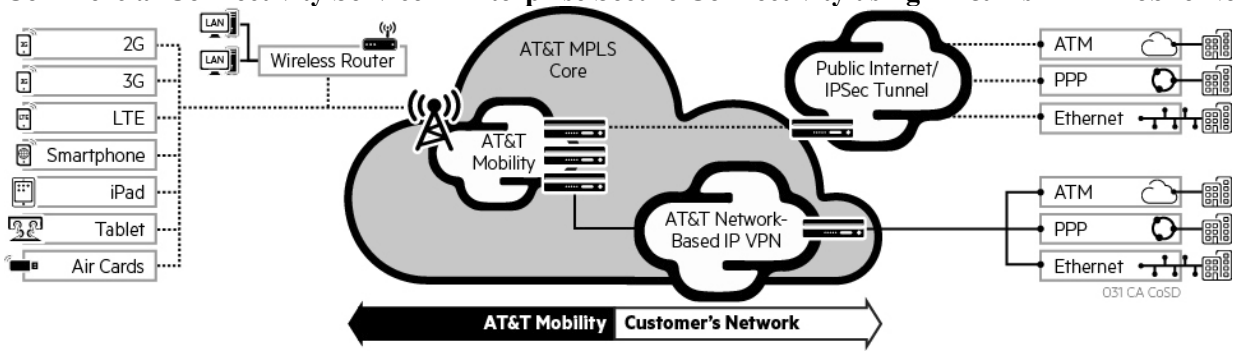
As identified earlier, T1 transport utilizing legacy TDM based connectivity, would be targeted for migration to ASE with NOD where possible. However, where fiber is not available without prohibitive construction cost, AT&T evaluates products such as copper-based AVPN that provides transport redundancy to the geo-redundant core. This service layers an AVPN service over a T1 copper circuit, providing AVPN cloud connectivity from a central office, creating pathway redundancy across the LAN. This solution continues to leverage the copper based wireline infrastructure that supports the site today, with a single point of failure still remaining on the "last mile"

of transport to the remote site. As Contractor evaluates its options for eliminating T1 sites these factors may drive Contractor to pursue other alternatives.

Such an alternative could leverage the AT&T mobility network infrastructure using Commercial Connectivity Services (CCS) over a private Access Point Network (APN) service. Using LTE/4G (or potentially even 5G connectivity as it is brought to market), this service allows for secure connectivity through Contractor's mobility infrastructure, to connect back into the County network's AVPN edge at the County Operations Center and AT&T POP. While this solution eliminates the "last mile" single point of failure, early deployments using the LTE network would need testing to fully assess the impact of potential latency issues. As Contractor looks further down the industry roadmap, advancements promised in 5G connectivity have the potential of providing a high speed, low latency service that could meet enterprise requirements.

Through a collaborative evaluation of these options, Contractor, in conjunction with the County, would develop a roadmap to migrate all T1 based technology to connectivity options which are in line with Contractor's geo-redundant core infrastructure. The figure below illustrates this concept.

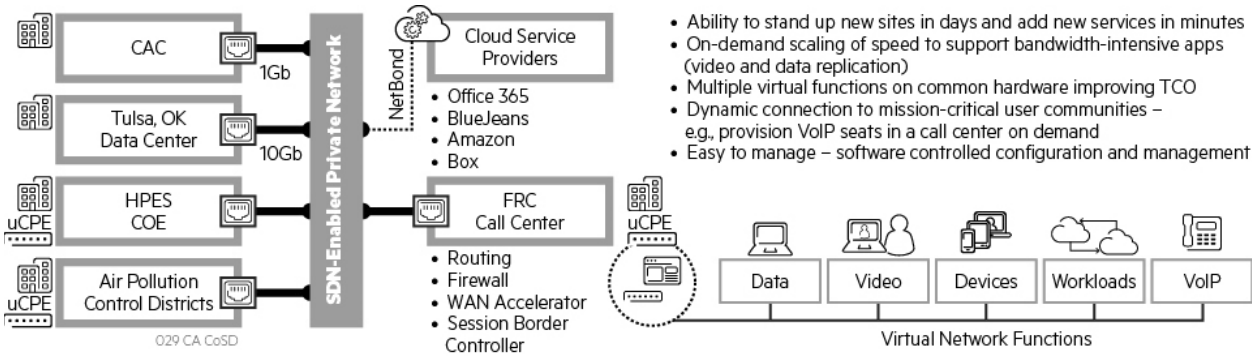
Commercial Connectivity Service – Enterprise Secure Connectivity using AT&T's LTE Mobile Network



Future Evolution of Software-Defined Networking-Based Services

During the life of the Agreement, AT&T would continually expand and improve its software-defined network (SDN) capabilities, where the local AT&T County network team would evaluate and recommend upgrades as they become viable and align with existing services. Midway through the Agreement term, Contractor anticipates key technical advances that could fundamentally affect the topology of the County network and the capital investment strategy. Building on the SDN foundation, new universal devices (Universal Customer Premises Equipment, or uCPE) could potentially represent a paradigm shift in how networks are provisioned and managed. Shifting capital cost to the provider, the County can take advantage of Network Function Virtualization, which provides services such as integrated LTE broadband backup, firewall, WAN optimization, and voice gateway functionality all on the same carrier managed device. Using Contractor's collaborative approach, Contractor would conduct production pilots, evaluate feasibility, determine business value, and make recommendations through the established Enterprise Architecture review process. The figure below illustrates the AT&T SDN enabled enterprise of the future.

AT&T SDN-Enabled Enterprise of the Future



As the needs of the County continue to evolve, Contractor would continue to collaborate with business unit and CTO staff and Contractor's cross-framework partners to understand the challenges and develop best-in-class solutions. Contractor believes that transformation is an iterative process, requiring strategic planning and vision coupled with practical approaches that ultimately make certain that functionality is provided to the customer in the most expedient way possible. Technologies identified in this solution are just the beginning of a contract lifecycle of change, but would provide a foundation for growth as Contractor moves forward as a trusted advisor to the County.

- Deployment plan for resources and use of facilities

The local, dedicated AT&T team—fully embedded in the solution lifecycle—provides all design, implementation, support, and monitoring of transformation activities. Technical personnel assigned to the County of San Diego and dedicated to the program are located at Contractor's Trade Street facility to maintain a fairly central base from which to service the County. All solutions leverage the AT&T Internet Data Center (IDC) in San Diego County as well as the County's Operations Center to hold the core hardware components and facilitate circuit terminations. Working from the local Trade Street facility, Contractor's SMEs would monitor, support, and maintain the remote services.

- Key methodologies and processes in solution

The local, dedicated AT&T team views transformation as an ongoing activity. By constantly monitoring what is currently available technology as well as keeping abreast emerging technology, Contractor is able to deliver concepts and ideas for consideration by the CTO. Contractor has already begun the task of installing ASE w/NOD at all new County sites; this task was preceded by the installation of two new host circuits, one each at the point of presence (POP) and County Operations Center (COC). Contractor would leverage this existing infrastructure as Contractor begins migration to ASE from the existing OPT-E-MAN connected county sites, with Contractor's project management staff coordinating the implementation(s). Work is also currently underway to consolidate the core GigaMAN backbone sites, with high-level architecture design already underway. The expectation is that the first two sites would be transitioned by approximately the end of the year.

Discussions with the County have already begun and are continuing related to cloud providers and the benefits that NetBond can provide. AT&T remains dedicated, so when and if the County decides this service is necessary—based on migration of various components to cloud providers and infrastructure—the local, dedicated AT&T team would bring in any resources needed to facilitate the entire process. This process would span final design and associated documentation, ordering of infrastructure components like circuits, and coordination with AT&T core services as well as cloud providers to provide a seamless transition. The local, dedicated AT&T team would continue to leverage all resources available within Contractor's local organizations (Engineering, Project Management, and Architecture) to provide all aspects of transition and transformation activities.

- Automated systems and tools involved in solution

The local, dedicated AT&T team uses a myriad of tools and automated systems to perform implementations and support operations and performance. These tools include Cisco Prime Infrastructure, the CA Spectrum suite, SNTC (Smart Net Total Care), Riverbed Cascade, and Panorama. Cisco Prime Infrastructure is used to centrally manage configuration as well as gather data related to changes, performance, inventory, and licensing. The CA Spectrum suite—which includes Spectrum and E-health—is used to monitor availability, performance, and inventory management; it also provides trending and analysis for traffic utilization. SNTC is a Cisco product used to manage support services as well as automate the process of gathering data for direct vendor support in the event of a problem. Riverbed Cascade is a deep packet analysis tool that uses NetFlow data, which is gathered passively and directed to it in an automated manner as well as active packet capture and analysis. Finally, Panorama is a Palo Alto Networks product that provides a central repository for logging, inventory of the Palo Alto components, licensing management, software image management, and analysis capability for the County security infrastructure.

Voice Services Transformation Project

- – Description of solution to meet the requirements

The solutions highlighted in this section include transformation initiatives planned for implementation early in the term as well evolutionary technologies that may arise later in the Agreement life cycle. Relative to statements focused on technology not yet available for deployment, AT&T would roadmap and evaluate the feasibility of these solutions during the Agreement life cycle. If identified as a viable replacement to existing services, AT&T would make recommendations for upgrades in line with refresh obligations or as otherwise agreed with the County.

AT&T's approach to transforming voice services focuses on enabling new features and capabilities used by both the End-Users and County constituents built on a foundation that is redundant, resilient, and highly available. The ultimate goal in developing the next architecture for voice services is to harden the core and edge locations and to offer robust and feature-rich UC for each and every End-User of enterprise voice services.

Core Network Transformation

Transformation activities at the Avaya Voice Core would migrate from any remaining traditional PBX architecture and provide an infrastructure reduction resulting in lower power consumption and reduced trouble tickets while minimizing disruption to users. This approach provides migration from the existing G650 Port carriers or other gateways, and upgrades them to G450 or G430 gateways. This transition would eliminate legacy IP Server Interface (IPSI) boards, mitigating risk by replacing end-of-life equipment and reducing the physical footprint in the data centers. This transition would take place at the Point of Presence POP as well as the County Operations Center (COC). In addition, the "TN" modules would be replaced with Media Modules in the G450s or G430s, and the digital signal processor (DSP) resources would be replaced with local media resources at the gateway as well as in the Avaya media servers.

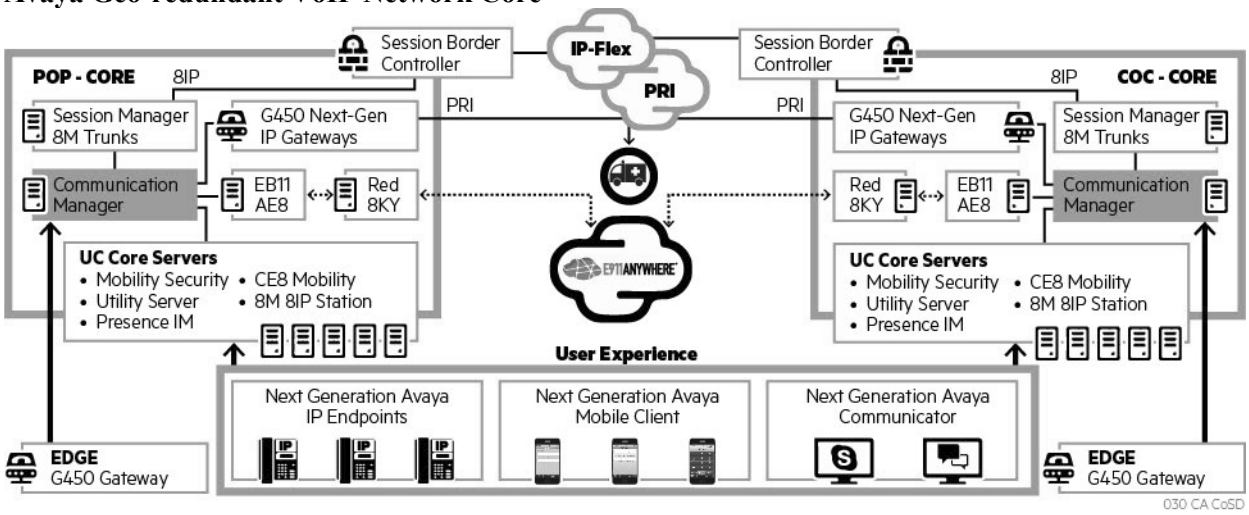
This highly available architecture would provide seamless failover between the COC and POP, with no single point of failure of the Core VoIP gateways. The architecture not only would provide centralized management between the two "Core" locations—POP and COC—but would also provide access to the remote locations, or locally survivable processor (LSP) sites.

Additional implementations would take place at the Core that would serve as the foundation for offering new and enhanced UC capabilities for End-Users, such as external mobile SIP endpoints on County- managed devices. This would be made possible by the Avaya Client Enablement Server as well as the Avaya Presence service for telephony presence on a mobile device.

Geo-redundant Voicemail

Contractor's solution includes the advancement and transformation of enterprise voicemail services, which replace the current, single-site-based voice messaging platform located at the AT&T POP, with a fault-tolerant, geo-redundant voice messaging platform located at the AT&T POP and COC. The new platform provides the ability for a standardized voicemail experience across all of the County's Avaya enterprise voice locations. This geo-redundant design incorporates live replication of the voicemail database, messages, and greetings between the AVST Call Servers at the AT&T POP and County Operations Center using AVST's never fail technology. The following figure illustrates the Avaya Geo-redundant VoIP Network Core. This solution is expected to be in place as the next agreement is signed. Using a roadmap strategy, AT&T Centrex users would be migrated over time to this platform, as specified below in the paragraph highlighting AT&T's Centrex migration roadmap.

Avaya Geo-redundant VoIP Network Core



The new platform provides the ability for a standardized voicemail experience across all of the County's Avaya enterprise voice locations.

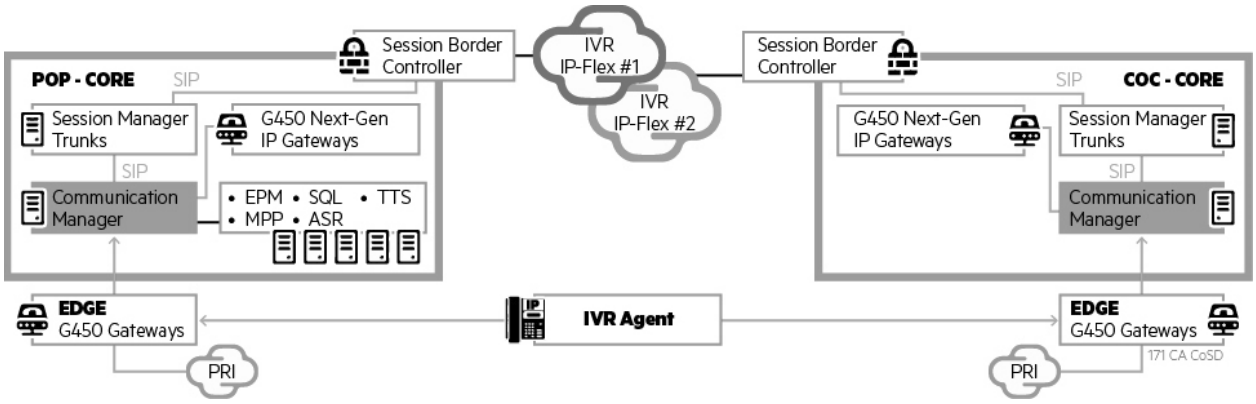
Interactive Voice Response (IVR) Transformation

Lastly, AT&T's transformation plan for Voice Services extends to Core adjunct services, such as its Interactive Voice Response (IVR) solution. The County's IVR infrastructure is built around the Avaya experience portal, which is a high availability contact center solution located at the AT&T POP. This platform provides access for external constituent service to County departments (such as Animal Services, Land Use Environmental Group, and various departments within the Health Human Services Agency) using features such as IVR, self-service, touch-tone, and speech recognition services. This scalable, high availability infrastructure provides many options for programming and agent integration, allowing customization for any type of constituent-facing contact center service.

The platform would undergo near term changes to external telephony connectivity as AT&T initiates plans to implement dedicated, fault tolerant inbound and outbound IP flex SIP trunks for the County's IVR infrastructure at the AT&T POP and County Operation Center. This change would prevent the Core IVR solution from impacting enterprise voice traffic, allowing business units to conduct high volume contact center activities such as outbound dialing campaigns. This new capability would provide a more standardized RU that business units can use to leverage the platform in meeting their business needs.

Over the term of the Agreement, AT&T would focus on roadmap initiatives and develop proposals to increase redundancy and resiliency of Core IVR applications as well as provide additional feature benefits such as automated agent call back and web chat.

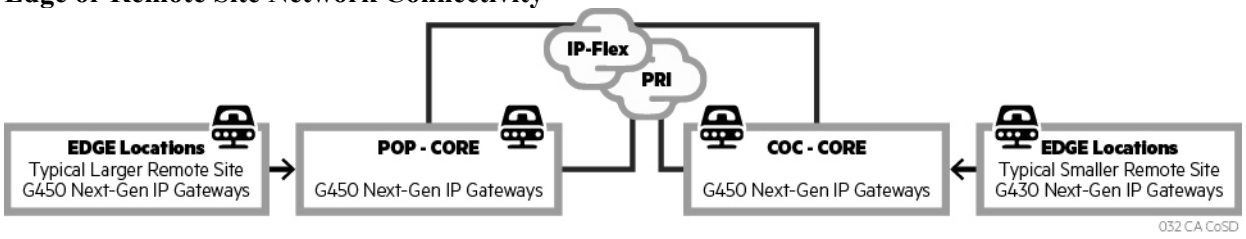
Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.



Edge Network Transformation

At the remote Edge, AT&T would replace all legacy cabinets and gateways (G650, MCC, SCC, CMC, and G700 series) with the latest generation of G450 or G430 gateways, providing LSP for resiliency. In the County, 81 sites have been identified as needing remote edge transformation to accommodate the implementation of VoIP phones. These 81 locations currently have digital telephones served from legacy cabinets and gateways. The Avaya G450 Media Gateway is a multi-purpose media gateway. The figure below**Error! Reference source not found.** illustrates Edge or Remote Site Network Connectivity. It works in conjunction with Avaya Communication Manager IP telephony software running on Avaya S8XXX Servers to help deliver intelligent communications to enterprises of all sizes. The G450 combines telephone exchange and data networking by providing public switched telephone network (PSTN) toll bypass and routing data and VoIP traffic over the WAN. The G450 features a VoIP engine, an optional WAN router, and Ethernet LAN connectivity. The G450 provides full support for Avaya IP and digital telephones as well as analog devices such as modems, fax machines, and telephones. Telephone services on a G450 are controlled by an Avaya S8XXX Server operating either as an External Call Controller (ECC) or as an Internal Call Controller (ICC). The G450 supports the Avaya S8300 Server as an ICC or, when the S8300 is installed in another media gateway, as an ECC. An ICC would be installed and used as a LSP. This is designed to take over call control in the event the ECC fails or the WAN link between the branch office and main location breaks. The LSP provides full-featured telephone service survivability for the branch office. The G450 itself also features Standard Local Survivability (SLS), which provides basic telephone services in the event that the connection with the primary ECC is lost.

Edge or Remote Site Network Connectivity



Centrex Migration

As detailed in the Voice Services section, the majority of voice services for the County are provided by the Avaya enterprise voice network. A small subset of the County's office sites does have voice services delivered by AT&T's Centrex business telephone service. Centrex service is typically deployed to smaller County sites that contain 1-20 users. At present, there are roughly 117 sites with Centrex voice services. While the AT&T Centrex business telephone services provide stable telephony and voicemail services, these locations are separated from

the remainder of the County's End-User population and are not able to take advantage of the full UC capabilities offered to Avaya enterprise users. With this in mind, the need to transform the features and capabilities for current Centrex voice services locations and to enable the users with the ability to use Avaya enterprise voice feature is a business priority. AT&T has developed a transformation approach to migrate a majority of these users' stations to a VoIP solution, while maintaining a roadmap for remote and intentionally off-net services to be executed during the term of the agreement.

The migration of Centrex users would begin with the deployment of stand-alone IP-based telephones at sites with existing data network functionality. This solution would provide services for VoIP telephone sets that is centrally managed by the Avaya geo-redundant voice cores at the AT&T POP and County Operations Center. While these sites would not have local survivable gateways, they would take advantage of the data network for their connectivity to the enterprise voice infrastructure. Of the roughly 117 Centrex sites across the County, 80 of these locations would be eligible for this service. Through this migration, over 65% of the Centrex remote sites and more than 272 individual stations would be converted to the Avaya enterprise standard. These sites/users would be provided new centralized voicemail and UC functionality as well as a new telephone set that leverages the County's investment in the data network for connectivity.

A greater challenge in the elimination of the legacy Centrex solution is associated with locations that do not have data network access. These locations are typically very small and remote locations that only require simple telephone service for communication. The migration of these services would be the topic of transformative roadmap planning during the term of the Agreement. Currently, AT&T is developing a Centrex replacement technology that is expected to provide transport and service options that would be evaluated for transformation. Some additional possibilities include the use of the mobility network for connectivity to the enterprise infrastructure, using an emerging technology called voice over LTE (Long Term Evolution).

Additionally, there are some remaining Centrex stations that have been placed throughout the County in locations with data network services where off-net phones are provided as a business requirement, such as elevator phones and emergency lines (red phones). As the Centrex replacement solutions mature, these solutions would also be evaluated for migration to a similar, off-network service so as to maintain the redundancy required for the specific use case.

VoIP Telephone Standard

The End-User experience is the single greatest change that would affect the County users in the proposed voice transformation. While the voice network is continually upgraded at the core, many telephone sets across the County have remained unchanged in over 15 years. By moving to new VoIP telephone sets, the County users would enjoy the benefits of a new device, along with improved reliability and performance.

There is significant value in resiliency that IP telephones offer over legacy TDM telephones. TDM devices require a dedicated port with a dedicated wire to connect to a local gateway. There are many points of potential failure, including the wire, gateway card, gateway power supply, gateway processor, and so forth. An IP telephone connects universally to any network port to facilitate registration to one of several points of call processing. An IP telephone would primarily be registered to the Session Manager Registrar at the core; there is a Session Manager Registrar at both core sites for high availability. In the event an edge location becomes fragmented from the WAN, the IP telephone would register locally to the G450 gateway with a local survivable processor (LSP).

Avaya/Skype for Business Integration

Another important pairing with a VoIP deployment is the implementation of E911 services. E911 allows for a continually managed registry of location data for each workstation so first responders have necessary information to effectively respond to an emergency call.

Another key End-User benefit associated with the Voice Transformation initiative is the integration of the Avaya enterprise voice system with Microsoft Lync (Skype for Business client). Using available licensing and open Application Programming Interfaces (API's), **Avaya Communicator** extends Avaya Aura real-time collaboration capabilities to Microsoft Lync 2010, 2013, or Skype for Business 2015, 2016 clients to provide users with a unified, consistent collaboration experience from their preferred applications and devices. The Avaya Communicator for Microsoft Lync service adds functionality to Microsoft Lync clients using only the Lync/Skype for Business standard client access license (CAL). Features include telephony presence aggregated with Lync's machine and calendar presence through Lync/Skype for Business client API and Lync/Skype for Business IM and desktop sharing, click-to-call control of PBX desk phones, voice and video, enterprise dial-plan support, toast pop-ups enabling incoming calls to be answered, and Reply with IM as well as a conversation window pop-up to access Avaya mid-call features and the ability through the Share My Bridge feature to launch a conference call and or collaboration session from within the client.

Avaya Collaboration Services

Avaya Collaboration Services interworks on the End-User PC with Communicator for Lync to provide UC services originated from Microsoft Office Suite, Outlook, SharePoint, and Internet Explorer as well as Mozilla Firefox and Google Chrome browsers.

When in Outlook or SharePoint, hovering over an End-User's name or presence indicator presents their contact details. The End-User now has the opportunity to IM, email, make a voice or video call, or schedule a meeting with this End-User. The End-User's presence is also displayed.

In addition, Collaboration Services would detect a number embedded in an email or a Word, Excel, PowerPoint, or SharePoint document and allow calls to be made to this number through Communicator for Lync. As with a call originated through the Lync/ Skype for Business End-User interface, a conversation window would be presented to provide the End-User with call control options for the duration of the call.

Collaboration Services automates the process of Join or Host a conference call. With this feature, the End-User can launch a conference call and/or a web collaboration session. The Collaboration Services would determine whether the End-User is the Host or a Participant to this call and uses the appropriate access passwords to access this call.

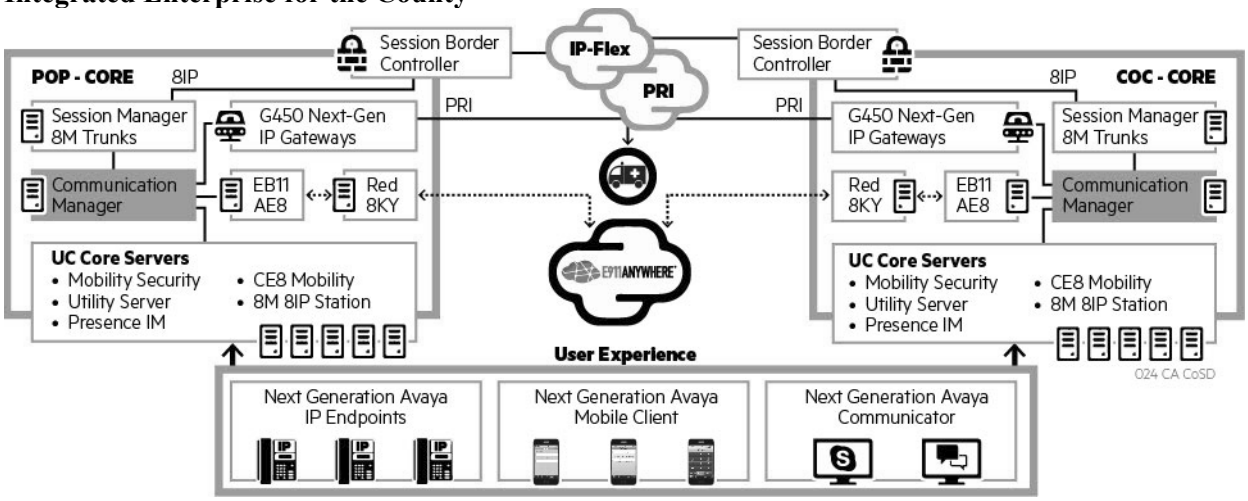
Collaboration Services, when used with Internet Explorer, Mozilla Firefox, and Google Chrome browsers, would recognize number patterns on web pages, and through the use of an intelligent algorithm applies enterprise, national, and/or international dialing rules to highlight these as phone numbers. These phone numbers can be dialed from a web site using the Avaya Communicator for Lync.

If a phone number is on an enterprise web page, Collaboration Services would take this number, access Active Directory, and pull down additional information for this End-User. This information is displayed on a contact card. The contact card is also populated with icons that enable the End-User to send an IM and see the presence of this contact, make a voice or video call to the contact, and schedule a meeting.

Integrated Enterprise Mobility

A final End-User benefit of the Voice Transformation initiative is integration of the End-User's voice and UC capabilities with their mobile device. Integrated Enterprise Mobility brings seamless interoperability with the desktop and desk phone. The figure below illustrates components of the County Integrated Enterprise experience.

Integrated Enterprise for the County



Integrated Enterprise Mobility brings seamless interoperability with the desktop and desk phone.

Features that span the desktop and desk phone are extended to the mobile End-User and are transparent in functionality. Examples include the following:

- Start a call from the County's desk (either desktop client or desk phone) and, if the County chooses to become mobile, simply select a button on the mobile app to move the call from the original location to the mobile device.
- Call processing from a mobile device extends a robust feature set (Hold, Transfer, Conference, Speaker, Mute, etc.) to the End-User so that transitioning from desktop or desk phone is seamless. The End-User experience is the same.
- The UC features of Avaya Communicator include visual voice mail to filter and sort voice messages. Use the visual voice mail feature to respond to important messages quickly. Communication History logs help the County traces the history of the County's enterprise calls and voice messages. Use Avaya Communicator to increase the productivity of the County's enterprise with tools that enhance collaboration, improve responsiveness, and lower costs for IT and End-User support.

- Deployment plan for resources and use of facilities

The local, dedicated team provides all the design, implementation, support, and monitoring of transformation activities and is fully embedded in the solution life cycle. Technical personnel assigned to the County are dedicated to the program and located at Contractor's Trade Street location, maintaining a central location from which to service the County. Additional leveraged resources may be engaged to support transformation and would operate under the direction of the local team.

All solutions use the AT&T POP as well as the County's Operations Center to hold the core hardware components and facilitate circuit terminations. All County facilities with voice network connectivity would house infrastructure and telephone sets necessary to provide service.

Key methodologies and processes in solution

The dedicated LCM team is embedded in the full life cycle of every enterprise voice and UC solution—from the initial gathering of requirements, through the design and implementation phases, to managing and monitoring, and even decommissioning when requested. Through customer meetings and service reviews, the team creates the proper solution that is chosen and sized appropriately.

Contractor would use standard Project Management methodologies in the scoping and execution of any new installation. AT&T architects and engineers would also use approved processes in their design and equipment placement activities. Enterprise voice and UC options are continually evaluated based on County business requirements in addition to current and emerging technologies.

Contractor's technical enterprise architecture team evaluates new products and standards to make recommendations to the CTO. When a recommendation is approved, Contractor's team moves forward with implementation recommendations including refresh of existing equipment and rollout schedules. For equipment issues, Contractor's Service Desk and engineering team work to identify and remediate the problem.

- Automated systems and tools involved in solution

To support quality voice service within the support levels defined by the new agreement, Contractor's subject matter experts (SMEs) use numerous automated tools. These tools enable Contractor to continuously monitor the overall health and performance of voice appliances, provide tools to assist in rapid restoration through fault isolation, and perform traffic analysis, as discussed below.

Contractor delivers complete manufacturer system maintenance coverage on all County Core Voice Services assets. The Avaya maintenance services include Avaya Expert Systems and Secure Access Link. Avaya Expert Systems provides the County Core Voice Services a maintenance database of more than 30,000 Artificial Intelligence Algorithms (AIAs) with scripted automation that is able to automatically correct many known system and software-related issues. Avaya Secure Access Link (SAL) is a centralized consolidation point for all Avaya Core systems for health and alarming monitoring, secure remote access using secure outbound-only HTTPS standards, and an integration point for Avaya Expert Systems. Together, these tools provide the County's Avaya Core Voice Services complete health monitoring and rapid issue resolution. Avaya Expert Systems and Secure Access Link are online and engaged 24/7 to diagnose and attempt to resolve known system alarms, clear many service-affecting issues, and escalate to engineering resources for prompt attention when necessary to allow service restoration or outage avoidance to County users.

Contractor's Voice Services team uses Nectar's Unified Communication Management Platform (UCMP) and leverages its complete suite of innovative features to provide the County enhanced integrated UC network services. Nectar provides multi-vendor management services including application dependency tree visual alerting and vendor knowledge modules, which assist Contractor's SMEs to proactively pinpoint and resolve cross-platform integrations issues to quickly restore services to County users. The UCMP also includes real-time network quality-of-service reporting using RTP (Real-time Transport Protocol) Control Protocol (RTCP) integration and can provide Contractor's team with the capability to create simulated traffic injection between designated network segments for analysis. This enables SMEs to monitor and report on all VoIP-related traffic transmissions. The quality-of-service reporting tool provides per-hop statistics, and in many cases assists in quickly identifying improper packet handling hop points, driving efficient resolution of network quality-of-service issues. The Nectar platform includes statistical resource utilization data gathering and storage that enables trending analysis and capacity planning so County users are not impacted by growing resource needs. Finally, all these capabilities are wrapped into an intuitive and customizable dashboard for use with visual and electronic alerting from sophisticated threshold configurations that drive the ability to acknowledge, respond to, and correct issues proactively in many cases before County users are aware of or report an issue.

E911 Manager would automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T MPLS network to track and update VoIP, digital, and analog phone moves, adds, and changes.

E911 Anywhere is a cloud-based 911 call routing service that can connect a 911 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada.

Storage Architecture Transformation Project

- Key Considerations and Potential Alternative Approaches

Architect Storage to Embrace Tiers of Well-Defined Storage: The solution being implemented by Contractor during the data center consolidation architects the design to embrace tiers of well-defined storage. The key considerations that went into the storage solution include cost and the ability to meet the County's requirement to keep the storage infrastructure current by refreshing storage components every 5 years. Contractor also considered the storage growth requirements and developed a solution with 20% year-over-year growth projected for the first 5 years.

In addition to Contractor's solution, which builds on the storage that is in place for the County on completion of the transition activities, Contractor considered two alternatives:

Storage Tiering Alternative: Contractor considered providing a 3PAR 20000 with 15,000 RPM drives and/or SSD as Tier 1, 10,000 RPM drives as Tier 2, and 7,200 RPM drives as the archive tier. This would provide a clearer delineation of the tiers from a performance perspective but would have resulted in a higher total storage cost than Contractor's actual solution. Contractor would continually monitor the performance of the storage environment.

Shared Storage Alternative: The second alternative is to provide storage as a leveraged service. This approach is similar to cloud storage in that the storage infrastructure would be shared with other non-County of San Diego clients, but the storage volumes would be dedicated to the County of San Diego. There would be no co-mingling of data on storage volumes, but the underlying storage hardware would be shared. All storage volumes would be securely wiped after they are no longer needed by the County, to prevent any chance of the County's data being exposed to non-County of San Diego customers on the leveraged storage infrastructure. This solution provides a lower cost per GB of storage. Using leveraged storage, Contractor could also provide the required tiers of storage using either the recommended solution or the Storing Tiering Alternative. However, with this leveraged approach, the County would not be able to specify the hardware refresh to meet their desired schedule, so Contractor rejected this solution.

- Description of solution to meet the requirements

Solution Summary: Upon completion of the data center consolidation, the storage architecture shall comprise a dedicated storage area network (SAN) with a 3PAR 20000 storage array in Tulsa providing tier 1, 2, and archive storage to all data center servers, consolidated in Tulsa. End-User data storage shall be provided directly from the new network-attached storage (NAS)-capable 3PAR. Otherwise, End-User data storage shall be the same. All 3PAR data shall be backed up locally using HPE Data Protector with a StoreOnce Virtual Tape Library (VTL) as the backup target. All backup data and disaster recovery (DR)-required 3PAR data shall be replicated to the DR site in Colorado Springs. The data center solution shall include immutable storage, which would also be replicated to the DR site. For the San Diego sites, backup data shall be replicated to the DR site instead of being copied to tapes, for remote offsite storage. Finally, the immutable storage refresh and reconfiguration shall be a newer version of the same immutable storage.

The Contractor's storage architecture following transition includes updated storage equipment, which shall be refreshed on a 5-year cycle. The storage array technology is flexible and efficient, designed to keep pace with the County's requirements as they evolve. Tiers 1 and 2 have been redefined to reduce cost without sacrificing performance. The backup solution would consolidate all of the County's backup needs into one capacity-driven solution that eliminates physical tapes from the environment. The location of the immutable storage solution would change with the Data Center Consolidation, and the hardware would be refreshed.

Contractor would continually evaluate the various storage tiers used by the County as their storage requirements evolve, with an eye toward providing the right storage solution for each tier. However, the storage solution that would be in place following Transition provides ample opportunity for growth in terms of storage and

performance, and achieve tier storage service is based on 3PAR 20000 storage devices—the latest innovation in 3PAR enterprise storage from HPE.

Contractor would continually evaluate the County's storage archiving needs and consider a cloud-based archive storage solution if/when cloud-based archiving meets the County's approval.

Rationale: The solution Contractor provides meets the County's post transition requirements and would allow the County to transform its storage architecture over time, as needed. The 3PAR is capable of supporting 15 PB of usable storage capacity. It would support a range of disk drive technologies from 7,200 RMP, 10,000 RPM, and 15,000 RPM Serial Attached SCSI (SAS) drives and solid state disk drives (SSD). The 3PAR supports storage migration without interruption via 3PAR-enabled storage peer motion (SPM). The 3PAR supports the following:

- Thin provisioning (TP), which is a method of optimizing the efficiency with which the available space is used in SANs. TP operates by allocating disk storage space in a flexible manner among multiple users, based on the minimum space required by each End-User at any given time.
- Auto tiering is a real-time intelligent mechanism that continuously positions data on the appropriate class of storage based on how frequently the data is accessed. This improves application performance.
- Compression, which reduces the number of bits needed to store or transmit data.
- Data deduplication, which reduces storage needs by eliminating redundant data. Only one unique instance of the data is actually retained on storage media.
- Federal Information Processing Standard (FIPS) 140-2—data at rest encryption to protect against loss or theft.
- Industry standard redundant array of independent disks (RAID) configurations to meet disk fault tolerance requirements and optimize performance.
- Remote and local replication for future refresh migrations on live data (meaning no down time required).
- Quality of Service to make certain bandwidth is available when needed.

The immutable storage solution has the capacity to support future growth in data storage requirements. The County's Document Processing Center (DPC) storage, which also uses 3PAR, would allow the DPC storage to evolve as needed. The direct attached storage would remain the same, and Contractor would continually evaluate services that use direct attached storage and work with the County to determine when/if those services can be migrated to SAN and/or cloud storage.

Timing: Contractor performs weekly reviews to assess capacity usage and determine whether changes are needed, taking into account any anticipated changes from the County.

Risk Considerations: This approach poses minimal risk based on continued use of the same platform. All capabilities are currently available, and the County can take advantage of this on a schedule that meets its needs.

- Deployment plan for resources and use of facilities

The Contractor's Storage Administration team would perform the assessments on an ongoing basis, as described above.

Storage hardware would be located in the Tulsa data center and at the San Diego sites, which include the DPCs at Lemon Grove and Viewridge. The storage would be replicated to the DR site in Colorado Springs.

- Key methodologies and processes in solution

At the 5-year refresh cycle, Contractor would continue to use replication extensively. Contractor's storage administration staff is well versed in array-based replication capabilities and would be able to extend replication to include the new hardware with little to no disruption to the County's compute services.

- Automated systems and tools involved in solution

Enterprise storage (3PAR) has native replication capabilities built in and enabled by the storage array software. The primary tool used to accomplish the storage transformation would be SPM. This type of replication is automated and keeps storage in sync on both copies of the data.

- Key Considerations and Potential Alternative Approaches

Classify County data and assign it to the appropriate tier: When evaluating solutions to classify County data, Contractor took the following items into consideration:

- The significant volume of the County's unstructured data currently stored in file shares, SharePoint, Exchange, and a range of other repositories; however, not all unstructured data is to be treated the same way.
- It is important to be able to classify data based on its importance, sensitivity, and need for access.
- By classifying unstructured data, Contractor can automatically direct it to appropriate data tiers to reduce storage costs while providing the County with the appropriate access requirements.

This initiative, is a primarily technology-driven effort coupled with consulting services to guide configuration of the solution. The alternative approaches are tied to specific implementation models for the various product suites that could be used to deliver this auto-classification.

- Description of solution to meet the requirements

Currently, a wide range of products is available to support the automatic classification of unstructured data/content. Through the application of policy enforcement, content can be targeted to different tiers of storage. The County has assessed a range of these products and has found several that appear to meet the requirements. Contractor would work with the County to design, configure, and implement the selected product suite.

Contractor would recommend, however, the County implement HPE's ControlPoint software. HPE is recognized by Gartner as a leader in Information Governance and Information Management (IM/IG). ControlPoint provides a robust platform for identifying, analyzing, and managing diverse types of information stored in enterprise repositories. Through continuous monitoring of enterprise repositories, ControlPoint can classify unstructured data based on a range of County identified metadata, including standard classification structure of Public, Sensitive, and Confidential documents, applying policy to facilitate optimal storage strategy.

Rationale: Applying file management tools would help the County to reduce its information footprint by identifying redundant, obsolete, and trivial (ROT) data; this can lead to reduced storage costs.

- Redundant data consists of duplicates such as unauthorized copies of documents, emails, records, or database information residing in file shares, SharePoint sites, mail systems, and databases.
- Obsolete data consists of information that is no longer in use or is out of date. Determining whether data is obsolete can be based on its creation date, last modified date, or access date; then assess this information in conjunction with an appropriate retention policy.
- Trivial data is determined by file type, where the file type has no content value, such as executables, system files, and thumbnails.

Additionally, such a solution can be used to tag and classify unstructured data, and through automatic application of policy, data can be targeted to specific tiers of storage or even deleted if appropriate. Ultimately this would lower the total cost of storage.

Timing: After completion of transition, Contractor recommends approaching unstructured data classification on an enterprise scale. Contractor's approach begins with an assessment and a pilot of a limited set of data/ repositories, while building out the required solution architecture to support the County's entire unstructured data

environment. Contractor's solution includes resources to manage the indexing of the remaining data, keep indexing up to date throughout the Agreement, and cross-train others on the support team.

Risk Considerations: Given the volume of data currently stored by the County, an enterprise-wide implementation can expose significant risk. Contractor mitigates the potential risk by starting the project with an early assessment to help define and test the County's data categories. Following the Milestones presented below also mitigates this risk through careful planning and testing prior to enterprise-wide rollout.

Key Dependencies: This solution is dependent on the availability of tiered storage architecture and file management/auto-classification platform, whether ControlPoint or an alternative selected by the County.

Milestones: Key Milestones for the data classification project include the following:

- **Milestone 1 – Develop Data Categories** – Building on the County's existing set of categories such as security classifications—Public, Sensitive, or Confidential—Contractor would use automated tools and common categories to develop a set of categories specific to the County. These categories could include County Groups, Function, and Availability. Contractor would select a set of representative documents from the County's data repositories to use for training and benchmarking. This makes certain that the categories created are based on meaningful concepts and real business context. This capability improves the efficiency and accuracy of categories and the application of policy to content. Preparation of theses draft categories would not affect documents in production systems.
- **Milestone 2 – Refine and Test** – This step helps to determine the relevance of the categories to enterprise documents. Refining a category is done by adjusting the weighting of a term or the selection threshold, or by adding field text. These activities can be done individually or in combination. A category can be published, making it available for use in automatic policy execution against content managed by the tool suite.
- **Milestone 3 – Auto-Classification** – Once County data is categorized; Contractor applies policies for ongoing management. Policies can be created with keywords, metadata, and/or example documents. Using the desired tool suite, Contractor can automate policy application, governing all aspects of the information lifecycle including deletion prevention, storage management, and ultimately disposition management by applying policies at data creation. Additionally, de-duplicating data across repositories helps to minimize storage costs and reduce discovery times.
- **Milestone 4 – Knowledge Transfer** – Following the pilot effort, further described below as part of Contractor's methodology and key processes, and validation of results, Contractor's subject matter experts (SMEs) would conduct knowledge transfer to the support team for the County to maintain the system and to index all County unstructured data.
- **Milestone 5 – County-wide Rollout**

- Deployment plan for resources and use of facilities

Contractor would initially provide a team of SMEs to guide the planning and piloting efforts. This team would work onsite, collaborating with the County's staff and the support team to define requirements and validate the results of the project. This team would also conduct knowledge transfer to facilitate extending the implementation and support County-wide. Contractor SMEs would remain available as required to provide reachback support. The infrastructure for the product of choice would be installed in the Tulsa Data Center.

- Key methodologies and processes in solution

A data classification project begins by working collaboratively with the County to gain insight and understanding of the legacy data landscape. This helps Contractor to define the benefits of a full legacy data cleanup solution, create a Solution Roadmap illustrating the go-forward plan, and implement the auto-classification solution infrastructure. Contractor then conducts a pilot, where Contractor would sample approximately 1 TB of data currently residing on the County's existing file share environments to determine appropriate classification structure and to demonstrate how data can be targeted automatically to different tiers of storage based on the

classification. Additionally, the assessment would showcase where unstructured data exists and how frequently is it being referenced/used so that intelligent decisions can be made regarding data management, archiving, retention, and retirement. Following the pilot, Contractor SMEs would perform knowledge transfer to the Contractor account team to facilitate indexing of the remaining data and then applying the solution to provide ongoing auto-classification of unstructured data.

- Automated systems and tools involved in solution

Contractor would use ControlPoint software or an alternative platform selected by the County to auto-classify unstructured data.

- Key Considerations and Potential Alternative Approaches

Develop Archival Solutions for Portfolio Applications: The County has more than 400 applications currently supporting its departments and citizens. These applications rely on different types of data—some unstructured, such as document management and SharePoint oriented data—and some with structured data. It is important to consider and evaluate the full portfolio of applications to determine the appropriateness of data archiving to reduce the data footprint and storage costs. There are two potential alternative approaches:

- **Approach 1:** Conduct an enterprise-wide assessment to determine the applications that are to be targeted for data archiving. Based on this assessment, develop an enterprise plan for rolling out the archiving capability.
- **Approach 2:** Start with a pilot effort to validate the cost savings that can be realized by application data archiving. Then conduct an enterprise-wide assessment and develop the roadmap for expanding data archiving.

Contractor recommends Approach 2 because this provides the opportunity for a quick win to both measure the impact of data archiving and to demonstrate its potential to support additional applications across the County. Also, it reduces the near-term investment in hardware and software. Finally, it helps to better define the County's true requirements, which reduces the potential risk of oversizing the enterprise archiving environment.

- Description of solution to meet the requirements

Contractor sees this initiative focusing primarily on applications that have structured, rather than unstructured, data sources. Recognizing that not all applications have the same potential for data archiving, Contractor would focus on database-to-database archiving as the primary archive model.

A component of the Contractor's Information Management/Information Governance (IM/IG) Portfolio is the Structured Data Manager (SDM) tool. SDM automates application lifecycle management and structured data optimization by relocating inactive data from expensive production systems and legacy databases, while preserving data integrity and access. SDM enables retiring outdated applications through an automated process of extracting, validating, and deleting data.

Rationale: This unique solution significantly reduces capital expenses and administrative costs, and helps the County to respond quickly to legal and compliance requests. This enables the County to obtain maximum value from the data.

Timing: This initiative can begin at any time after Contract Effective Date (CED); however, Contractor recommends beginning this initiative after completion of Transition. This would make sure that all changes to the data center architecture are complete and would reduce the complexity of implementation.

Risk Considerations: Each application would have to be assessed and evaluated independently to determine the value of archiving data. There is a risk of overestimating the impact of application data archiving, leading to over-solutioning the archiving platform. Contractor addresses this risk by starting with a pilot effort for a single application that meets a common profile for successful archiving. Contractor would also assist the County to assess other applications and prioritize them for archiving based on the potential for storage or other savings.

Key Dependencies: There are no real dependencies—in fact, the County considered a pilot effort in 2015. However, as stated above, Contractor would recommend delaying the start of this initiative until after completion of the Transition phase of the Agreement.

Milestones: Key milestones for this initiative include the following:

- Milestone 1 – SDM Requirements and Analysis
- Milestone 2 – Architecture and Solution Design
- Milestone 3 – Foundation Build in Development/Test Environment
- Milestone 4 – Onboarding and Archiving of the Central Reporting System (CRS) Tax Data
- Milestone 6 – Knowledge Transfer and Testing
- Milestone 7 – Foundation Build in Production Environment
- Milestone 8 – Post Production Support and Documentation

- Deployment plan for resources and use of facilities

Contractor would initially provide a team of SMEs to guide the planning and piloting efforts. This team would collaborative onsite with the County's staff and the local support to define requirements and to validate the results of the project. The team would also conduct knowledge transfer to facilitate extending the implementation and support County-wide. Contractor SMEs would remain available as required to provide reachback support.

- Key methodologies and processes in solution

The County has in excess of 400 applications. The potential value for archiving portfolio data varies significantly from one application to another. Contractor recommends conducting a pilot effort on one of the County's applications to validate the potential for reducing application data storage requirements rather than starting with a County-wide implementation of Portfolio Application Archiving.

Previously, the County, with the support of Contractor, identified Treasurer-Tax Collector (TTC) CRS as a candidate for the pilot effort. Following the pilot, Contractor would work with the County to develop a strategy and roadmap for extending application data archiving to other County applications.

- Automated systems and tools involved in solution

Contractor plans to use the SDM tool, described above, to reduce the data footprint of the County's structured data. SDM software comprises an integrated set of components that facilitate design, deployment, and ongoing management of archiving processes throughout the lifecycle of applications and data. In addition, they deliver capabilities that address different levels of application complexity, data volumes, and archive access requirements. The components include the following:

- Designer – Provides a visual interface to model data and create business-aligned data migration rules with ease
- Data movement – Makes sure data relocation is performed to meet volume requirements while retaining application integrity at all times
- Archive access – Provides a full range of access capabilities to meet requirements for business operations, regulatory compliance, and legal discovery
- Job engine – Automates all archiving tasks with built-in recovery and restart
- Management console – Provides system configuration, job monitoring, job launching, and complete audit trail capabilities

- Key Considerations and Potential Alternative Approaches

Hyperconverged Integrated Systems: Hyperconverged infrastructure is designed to simplify the design and management of the computing environment by merging and pre-packaging the server, network, and storage components of infrastructure into pre-sized building blocks. To deliver the most value, hyperconverged systems would have to comprise nearly all of the infrastructure deployed in the data center; otherwise, the hyperconverged

solution becomes just another platform that has to be integrated and adapted to existing standards; this would increase rather than decrease overall complexity in the environment.

One possible application of hyperconvergence that the County could consider in the shorter term would be the implementation of hyperconverged infrastructure for servers deployed in County field sites. As systems come up for refresh, Contractor would compare available options in the marketplace for cost, compatibility with established management tools and fielded applications, and if a hyperconverged solution would yield benefits to the County, Contractor would recommend its implementation.

- Description of solution to meet the requirements

Contractor would implement Helion MPC and Helion Managed Cloud Broker (HMCB) during the Transition as Contractor builds the County's on-demand Dev/Test and Production environments as part of the data center consolidation. These platforms start the County on a path of greater standardization in the virtual/converged infrastructure environment. By implementing a private cloud with standard-sized building blocks of virtual infrastructure, Contractor would be able to test and validate whether a hyperconverged infrastructure would ultimately yield benefits for the County.

When the County is ready for hyperconvergence, Contractor would provide the technology partnership to achieve this. If Contractor is able to fully standardize over time on the x86 platform in the converged infrastructure, then the next logical step is to plan, design, and implement a hyperconverged infrastructure. During the planning phase Contractor would build the business case for hyperconvergence and would provide the County with alternative solution designs built on the most suitable and current technology and vendors available. HPE offers a wide range of hyperconverged systems that Contractor continues to advance and innovate with to suit various business cases and client needs.

To achieve the best possible outcomes from the County's investment in this technology and to meet its needs in a way that helps to better support County business, Contractor would consider and evaluate the following features to help the County select the optimal hyperconverged solution:

- **Integration for Seamless Coexistence**. Ability of the hyperconverged solution to integrate with the legacy environment. The hyperconverged solution must enable the County to fully integrate the new solution with the legacy environment. Existing server and storage assets must be able to coexist with the new environment until the eventual collapse of multiple administrative interfaces into fewer simpler tools.
- **Scalability**. Ability to grow the environment in a non-disruptive manner and the ability to scale up or scale out without replacing the initial equipment with new equipment. The solution must offer just-in-time growth capability to avoid the need to carry expensive inventory. Additionally, granularity in scalability is important to scale only the resources required in the increments that make sense for the County.
- **Data Mobility**. Ability to move data around to accommodate individual device outages—the ability to easily move data between the hyperconverged platform and other systems, without having to rely on consultants.
- **Data Protection**. Ability to protect data in the event of hardware failures, human error, or natural and manmade disasters while meeting desired SLAs, RPOs, and RTOs without the need for an additional software or hardware layer. Features Contractor would evaluate for the County include RAID or mirroring, fault tolerance, replication (synchronous and asynchronous) within the site and between sites as well as full disaster recovery capabilities.
- **Performance**. Ability to provide performance opportunities that are considered enterprise-class. This means that the solution is to support flash and, optionally, spinning disk. Ideally, both would be supported because they have different strengths and weaknesses. When it makes sense, the solution should be able to automatically tier storage systems to enable faster data access or, at the very least, have an accelerated method for handling data retrieval.

- **Availability**. Ability to provide availability at SLA levels that meet County requirements for all systems. To determine this, Contractor would evaluate ease of scalability, ease of management, ability to scale out storage, tolerance for node loss, cluster resiliency, and capabilities of automated failover.

Once Contractor has identified and received County approval of the plan, in a parallel but fully integrated mode of operation Contractor would execute a phased migration of the County's systems to the new hyperconverged infrastructure. Contractor's plan would also consider data center component refresh dates to maximize investments in the legacy environment prior to the migration.

Timing: Preparation for implementation of a hyperconverged infrastructure would occur during transition. Contractor recommends the actual implementation to occur as data center components come up for refresh.

Risk: None at this time.

Dependencies and Milestones:

- Prior to the County investing in a hyperconverged integrated solution, standardization on the Managed Private Cloud platform must be established
- To migrate to a hyperconverged infrastructure, existing legacy equipment would need to be refreshed onto the hyperconverged platform.
- Development of implementation strategy and plan.

- Key methodologies and processes in solution

With the implementation of hyperconverged systems, methodologies and process for deployment become easier as a result of the pre-configuration of server, network, and storage components of infrastructure into pre-sized building blocks. These systems include easy-to-use management tools designed to streamline implementation and management and help shield the administrator from much of the underlying architectural complexity.

Contractor's new hyperconverged systems deploy VMs in just five clicks, update hardware and firmware in just three clicks, and provide instant diagnostics and analytics to enable faster response to business needs.

- Deployment plan for resources and use of facilities

Contractor's facility approach is to deploy the new hyperconverged infrastructure at Contractor's primary data center in Tulsa, Oklahoma and/or in field sites as deemed appropriate.

- Automated systems and tools involved in solution

Contractor's vision is to dramatically simplify and streamline IT administration and operations management. While many hyperconverged integrated system solutions are available on the market today, Contractor is a market leader in hyperconverged systems. Contractor's hyperconverged systems offer an infrastructure that provides the following features/benefits:

- Rapid provisioning of VMs
- Flexibility and speed to add capacity in as little as 15 minutes
- Simple IT operations with firmware and driver updates in just three clicks
- 99.999% continuous data availability
- Federated lifecycle management
- Data fabric with data mobility across systems, sites, and cloud
- Lower startup cost with two-node entry and linear scaling
- 62% lower cost for disaster recovery
- Pay-as-you-grow flexible capacity model

Using HPE OneView as the common software-defined convergence platform, Contractor provides software-defined management for both Contractor's larger ConvergedSystem 700 powered by Intel models as well as the smaller CS200-HC models. The HPE OneView End-User experience (UX) makes managing and monitoring systems so easy, no manual is required. HPE OneView integrates with HPE Helion OpenStack and CloudSystem and has extensions to a variety of management software. With a commitment to provide clients with the most flexibility, Contractor has been continually and significantly expanding this ecosystem since 2015.

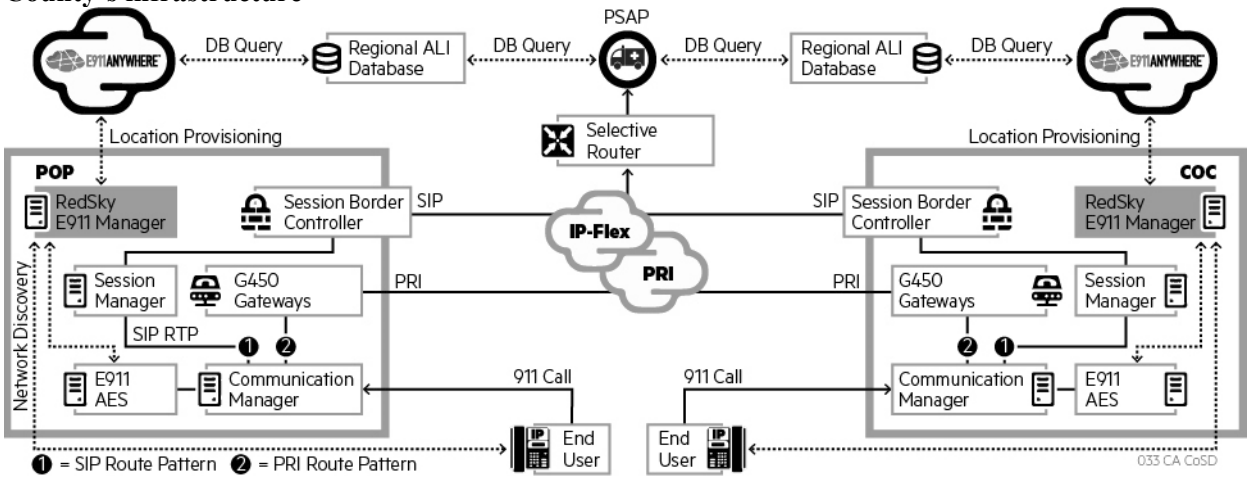
E911 Transformation Project

- Description of solution to meet the requirements

The solution highlighted in this section specifies the E-911 migration planned for implementation early in the Agreement at existing VoIP sites and ongoing in parallel with VoIP site upgrades.

Contractor recommends the adoption of the industry leading E911 Manager and E911 Anywhere by RedSky technologies. RedSky's E911 Manager® solution would be implemented in line with the County's geo-redundant network core, with infrastructure at the AT&T Point of Presence (POP) and the County Operations Center (COC). The primary application would run on an active host with a standby host that would take over in the event of failure of the primary server, enabling full redundancy.

Fully-integrated E911 solution would automate the E911 process by recognizing route patterns within the County's infrastructure



The E911 Manager would *automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager via the AT&T MPLS network to track and update phone moves, adds and changes.*

To handle the growing deployment of VoIP services throughout the County, RedSky's E911 Manager would communicate with the Avaya Enterprise voice network to monitor registration events of VoIP endpoints. E911 Manager would use Layer 2 Network Discovery or Layer 3 Network Regions to determine the location of the End-User based on port, network device, or IP address and would update the Avaya Communication Managers with the proper Emergency Line Identification Number (ELIN) for 9-1-1 off-net calling. The E911 Manager server would create and store Automatic Location Identification (ALI) records as necessary and submit to RedSky's E911 Anywhere® cloud service in the required format for the local Public Safety Answering Point (PSAP).

To manage ALI information centrally—for County locations or to support mobile softphone users—the RedSky solution includes RedSky E911 Anywhere cloud service. E911 Anywhere is a cloud-based 9-1-1 call routing service that can connect a 9-1-1 call to more than 6,000 PSAPs in the USA and Canada. E911 Anywhere is an

effective choice for the County based on its distributed locations as well as the increase in mobile and desktop IP softphone users. The recommended solution by AT&T would feature the following:

- A fully automated E911 solution that would track the location of phones as phones move within the County's enterprise voice network
- An E911 software application located at the AT&T IDC and COC that would interface with the Geo-Redundant Avaya Communication Manager voice network
- A solution that connects with all Private Switch-Automatic Location (PS-ALI) Identification databases throughout the cities within the County
- A solution that provides Emergency On-Site notification to anyone working at the County of the location of a call placed to 9-1-1
- Geo-Redundant Active / Active Server construct located at the AT&T Internet Data Center (IDC) and COC for high availability and redundancy
- Reporting and metrics for auditing of all E911 activity
- As a "cloud-based" 9-1-1 call routing service, E911 Anywhere can send a 9-1-1 call to any PSAP in the U.S. or Canada (with County approval)

E911 is a necessity for the County enterprise VoIP deployment. As stated in the introduction, this solution would be integrated into the County's enterprise-wide VoIP migration, enabling functionality on a site-by-site basis over the length of the transformation initiative.

- Deployment plan for resources and use of facilities

For the e911 solution, Contractor shall ensure that AT&T leverages the local LCM (Life Cycle Management) team, in-house vendors, direct manufacturers, and carriers. Contractor shall ensure that AT&T personnel provides this support from its location on Trade Street in San Diego.

- Key methodologies and processes in solution

All support services—whether triage, new requests, change requests, or removals—are initiated by the County End-User to the Contractor Service Desk. All requests within the network framework for E911services would be directed to the AT&T LCM team for assessment and completion.

AT&T would leverage the RedSky's solution for updates to the PSAP routing and PS-ALI databases as County staff request Adds, Moves or Changes to their VoIP telephone stations. The tracking of VoIP phones is made possible by enabling Layer 3 Network Regions on the County's LAN. This is the most common method of tracking IP, SIP, and IP soft phones inside an enterprise. This method, which is specific to Network Regions or subnets, establishes a dedicated block of IP addresses associated to the region at the DHCP server. Each Network Region would then have assigned to it a physical address and an ELIN. Every time a VoIP phone registers to the Avaya Call Manager at the AT&T POP or County Operations Center, E911 Manager reviews the IP address of the VoIP phone to determine if the IP address falls into one of the IP address ranges set aside for the regions. If E911 Manager determines that a VoIP phone is in a Network Region, E911 Manager would provide the ELIN to the respective Avaya Communication Manager server at the AT&T POP or County Operations Center.

- Automated systems and tools involved in solution

E911 Manager solution would automate the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T Multiprotocol Label Switching (MPLS) network to track and update VoIP, digital, and analog phone moves, adds, and changes.

E911 Anywhere is a cloud-based 9-1-1 call routing service that can connect a 9-1-1 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada.

Identity Federated Services Transformation Project

- Description of solution to meet the requirements

Contractor analyzed Okta, Oracle, and IAMaaS during the technology selection stage and recommended HPE's IAMaaS due to the maturity of the product and services, purchase and maintenance cost, and lower risk during implementation. However, if the County opts for another solution such as Okta or Oracle, Contractor would work with the County to plan and execute a successful implementation of either vendor's solution.

The recommended Identity Federated Services solution includes the following components:

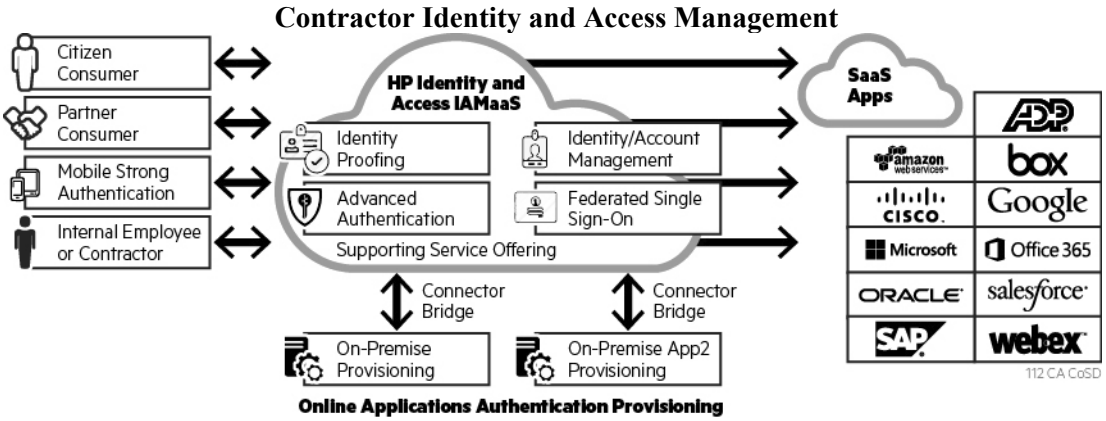
- The existing Oracle IDAM technology platform as its core
- Microsoft Active Directory Federation Services (ADFS)
- HPE's IAMaaS to enable the federation services where the County is acting as service provider and identity provider.

Contractor would use IAMaaS to integrate external constituents within the County's Identity Management Service. IAMaaS is a cloud-based IDAM) solution built using the Computer Associates (CA) secure cloud product for multi-tenancy. IAMaaS is hosted on the HPE Helion Managed Virtual Private Cloud for U.S. Public Sector. The following elements describe the main features of the IAMaaS solution and how they relate to the County:

- User life cycle management such as self-registration, password resets, and profile updates.
- Application access management to request access to applications.
- Hybrid provisioning cloud and on premise to create/update on-premise identity requirements.
- Identity synchronization on premise to make certain that relevant data is updated one way or bi-directionally.
- Reporting for compliance and audit.
- Identity proofing from the solution to County data stores.
- The single sign-on (SSO) Federation Hub can act as identity provider (IDP) and service provider (SP) to County software as a service (SaaS) applications.
- IAMaaS can act as a Federation Hub. External users can be authenticated to SaaS apps using their County/IAMaaS credentials, County credentials, or social login credentials like Facebook.
- The CA Security SaaS Validation Program helps SaaS vendors increase sales and adoption by simplifying and validating their SSO interoperability. It enables smooth integration of SaaS solutions into CA SSO environments in an End-User-friendly and cost-effective way.
- Credentials may include Forms, Integrated Windows Authentication (IWA), multi-factor authentication (MFA), public key infrastructure (PKI), Radius, OAuth, one-time password (OTP), and Risk.

The figure below illustrates the main elements of the IAMaaS solution and its relationship with the County, its citizens, employees, and partners. On the left side is each type of End-User who would interact with the service. Within the core or "cloud" of IAMaaS are the key services provided such as identity proofing, identity and account management, federated SSO, and advanced authentication. The resources and services to access are on the right; those services are both internal and external to the County IT environment, including third-party providers. Connectivity to the resources via the IAMaaS are enabled via industry-standard IDAM protocols.

IAMaaS solution



Providing secure IT services operations through robust End-User identity authentication.

Rationale: Contractor believes that expanding the current IDAM capability along with implementation of HPE's IAMaaS for identity management of external users provides the most cost-effective solution. This approach *provides a low risk, non-disruptive method* to expand on existing County investments and meets the County's architecture vision for identity management.

Timing: The timing for expansion of the existing County IDAM solution to include federation would coincide with the ConnectWellSD project or other timing as required by the County. Other elements of the solution such as federation requests to business partners would occur as the solution is deployed.

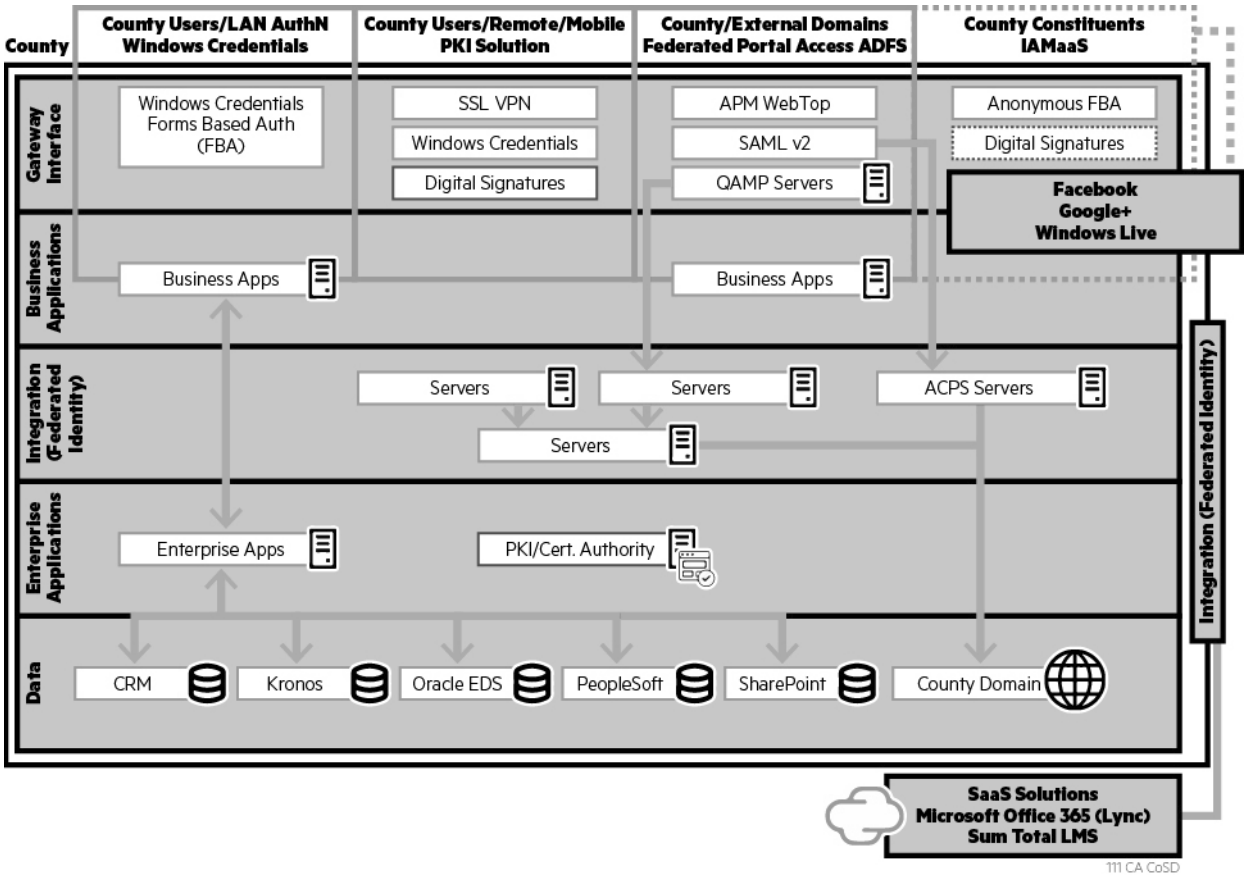
The figure below depicts the overall view of the IDAM solution and how Oracle, ADFS, and the HPE's IAMaaS would work together to provide identity federation. As seen in the figure, the core elements of the IDAM solution would work together to enable seamless federation between the County and third-party providers, external State and Federal agencies, and identity management for County residents.

The County ADFS 2.0 environment—a key component of the Identity Federated Services—has been operational since 2011, providing secured identity federation and web SSO capabilities for County and external business unit End-Users who require access ADFS-secured applications within the County network and in the cloud.

Earlier in 2016, the ADFS environment was upgraded to v3.0 with redundancy, and included a new test environment. By adding external access to the test ADFS server, this upgrade provides expanded use of the ADFS test environment for development and testing of new ADFS-secured applications.

Upgrading the ADFS environment was part of the County's overall IT roadmap to refresh and improve key infrastructure components and expand the County's IDAM solution. The key point is that this solution is strongly tied to the Identity and Access Management Services solution; it is a continuation of that capability but expanded to enable federation—much of the approach is duplicative.

The IDAM solution integrates Oracle, ADFS, and the HPE's IAMaaS



This solution offers minimal risk to the County and enables seamless federation between the County and third-party providers, external State and Federal agencies, and identity management for County residents.

Key Dependencies and Milestones: As a part of the overall IDAM effort, Identity Federated Services is encapsulated in the following list, which details the progressive steps of the IDAM solution and details what is being done today and what Contractor would perform in the future:

- Current/on-going effort – Oracle Federation Manager is currently deployed with Service Provider active and Identity Provider not active. Based on an existing request from the Department of Child Support Services (DCSS), Contractor plans to implement the Federation Acting as Identity Provider upon approval. To deliver the federation capability for DCSS, IAMaaS needs to be implemented simultaneously with Federation Acting as Identity Provider.
- Future – Develop a process for auto-onboarding new employees based on the information in PeopleSoft to create the Active Directory (AD) identities
- Future – Expand use of the existing platforms into all County business units and partners as well as work with the current Knowledge Integration Project (KIP) team (IBM) to expand to partners
- Future – Use Contractor's IAMaaS solution to expand to County residents and to act as the identity manager for County residents
- Future – Re-architect the solution to become a zero downtime solution
- Future – Federate with County third-party vendor applications

- Deployment plan for resources and use of facilities

Ongoing support for the IDAM service would be delivered by continental U.S.-based delivery resources in line with the County's requirements. With more than 5,000 security professionals who have IDAM expertise, Contractor has the experience to deliver even the most complex solutions.

The Contractor Tulsa Data Center would be the production data center, with the IDAM solution delivered from this location. This includes almost all web, application, and database servers, data storage, and data management. The Contractor disaster recovery (DR) site in Colorado Springs would provide the recovery site for the IDAM solution.

- Key methodologies and processes in solution

Contractor would adhere to the following key processes to deliver Identity Federated Services:

Solution Methodology: By incorporating the Contractor's IT Strategy & Architecture (ITSA) for Identity Federated Services, Contractor would take the same iterative approach, addressing issues and improvements in data quality and data management—in both practice and implementation. Through this process, Contractor would work closely with County data teams and other Contractor Transformation, Integration, and Architecture (TIA) data architects to define and manage County IT outsourcing enterprise data semantics. ITSA for Identity Management advocates a rapid, incremental, and iterative approach that can be aligned with the County's hybrid development methodology.

In addition to the ITSA, Contractor would use standard TOGAF (The Open Group Architecture Framework)-based architecture approach to develop the solution artifacts and produce the required documentation to make certain that the solution is documented correctly and that it also would lower the overall implementation risk to County. Contractor would integrate these key methodologies with the County's current Architecture and Solution reviews in conjunction with the County Technology Office (CTO) and relevant County groups.

For the Oracle IDAM Suite, Contractor would work with Contractor's IDAM architect to make certain that the design, development, and deployment of the Oracle suite follow standard Oracle design and deployment methods. This would facilitate operation of the Oracle platform within the design parameters. Any significant design changes to the platform or changes to the Oracle databases would follow Oracle mandated practices.

- Automated systems and tools involved in solution

Contractor would use the Oracle and Microsoft tools identified in the table below in support of Identity Federated Services.

Automated Tools for Support of Identity Federated Services

TOOL	PURPOSE
Identity Manager	• Oracle Identity Manager is designed to manage End-User access privileges across all of the County's resources, throughout the entire identity management lifecycle—from initial creation of access privileges to dynamically adapting to changes in business requirements. Identity Manager enables the incorporation of necessary business changes at minimal cost, while avoiding enforced customization.
Access Manager	• Oracle Access Manager provides adaptive authentication, federated single sign-on (SSO), risk analysis, and fine-grained authorization extended to mobile clients and mobile applications. Services can be licensed and enabled as required to meet the specific needs of the County.

TOOL	PURPOSE
Federation Manager	• Oracle Identity Federation (OIF) provides secure identity information exchange between external/internal partners. OIF provides account management for partner identities and integrations through support of industry federation standards. OIF protects existing IT investments by integrating with a wide variety of data stores, End-User directories, authentication providers, and applications.
Virtual Directory, Unified Directory	• Oracle Virtual Directory provides Internet and industry-standard Lightweight Directory Access Protocol (LDAP) and eXtensible Markup Language (XML) views of existing enterprise identity information without synchronizing or moving data from its native locations.
Microsoft tools and services also be used: • Microsoft Active Directory 2012 • Microsoft ADFS	• Microsoft Active Directory (2012) Domain Services (AD DS) provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications. Administrators can use AD DS to organize elements of a network—such as users, computers, and other devices—into a hierarchical containment structure. The hierarchical containment structure includes the AD forest, domains in the forest, and organizational units (OUs) in each domain. • ADFS (Active Directory Federated Services) provide County users with SSO access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and to implement federated identity. (Claims-based authentication involves authenticating an End-User based on a set of claims about that End-User's identity contained in a trusted token. Such a token is often issued and signed by an entity that is able to authenticate the End-User by other means, and that is trusted by the entity doing the claims-based authentication.) It is part of the AD DS.

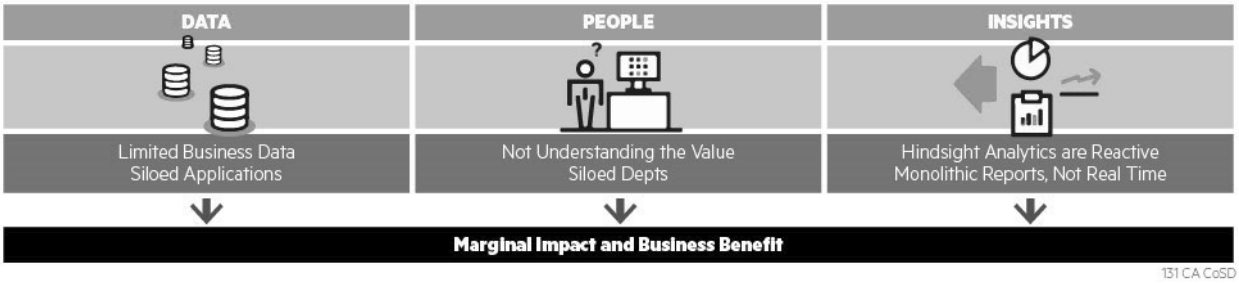
Enterprise Information Management Transformation Project

- Key Considerations and Potential Alternative Approaches

Contractor recommends implementation of an Enterprise Information Management (EIM) program to capitalize on the valuable data that is available but currently not harnessed. This shall provide the County with information it needs to make more informed decisions and present an enterprise view of the data that could be used to make richer programs available to the public.

The County has begun the journey to modernize the Information Architecture and Governance model a critical step as modernization and transformation of the IT infrastructure begins. The information architecture must address traditional "feeds and speeds," and include business definitions of information and the information processes to incorporate all data (structured, semi-structured, and unstructured (xml, flat files, scanner files).

Siloed business data, as shown in the figure below makes it difficult to take full advantage of the information available across the enterprise. To the County, this could mean employees are limited in their ability to perform certain job functions or provide the services citizens need. This can result in added frustration for both employees and citzens.



When data is siloed, it is more difficult and time consuming for County employees to find the information needed to support citizens.

EIM provides an essential framework for managing and governing information (data) across the enterprise and requires:

- Governance and stewardship
- Integration
- Methodologies and standards
- Architecture and technologies
- Enterprise data models

The payoff for an EIM solution is clear—the County would be better prepared to more rapidly meet the needs of employees and citizens by gaining greater insight from the data it collects, as shown in the figure below.

Integrated Data Across the Enterprise.

Easy access to all available data facilitates decision making and helps to achieve superior business outcomes.

As Contractor and the County develop a modernized Information Architecture and Governance model, Contractor would consider a wide-range of common challenges that include:

- Inconsistent definitions of key business data, leading to incomplete, incorrect business metrics
- Information that is not available, incomplete, inaccurate, and untimely to enable informed business decision
- Time-consuming, manual processes, adding to employee workload and citizen frustration
- Fragmented data, preventing or delaying comprehensive situational analysis and appropriate actions
- Siloed project work, preventing integration or extension across enterprise
- Inconsistent data, preventing standardization and reuse of processes, methods, among others
- Siloed decision making, which may be counterproductive to the enterprise
- Poor data quality and fragmented data security/auditability, exposing compliance risks (SOXA, HIPAA, ISSA, CCA, FRCP, Basel II Accord, PCI, EU Privacy Directive, etc.)
- Unknown data retention needs/requirements, transforming data assets into data liabilities (storage costs & exposure risks).

Contractor recommends EIM for developing a coherent and supportable Information Architecture and Governance model. This approach would focus on developing an information strategy and a roadmap for implementing the strategy, and then to invest in delivering the supporting initiatives.

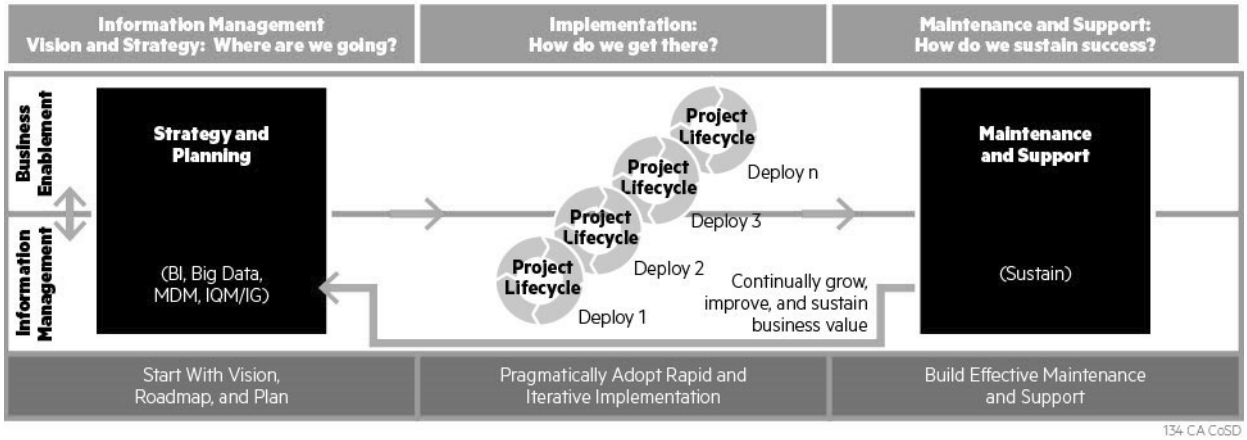
- Description of solution to meet the requirements

Contractor proposes a two-phased approach to establish a coherent EIM program. The first phase is a stand alone project. This project focuses on the objective defining the County's EIM program. Key deliverables from this project include: Vision and Strategy Document and EIM Roadmap.

The second phase is would consist of a number of separate projects detailed in the Roadmap from Phase 1. Each project would have well defined objectives and deliverables defined throughout the implementation process. Specific intitiatives/projects identified in the roadmap are executed in a rapid and iterative approach. Contractor scopes the implementation projects upon completion of the vision and strategy. Projects associated with the second phase would be completed via work request.

The figure below illustrates the Contractor approach to EIM. Of particular note, Contractor's approach is to address and align business enablement with information management.

Contractor Approach to EIM



Contractor's approach aligns business enablement and information management that address true business needs.

Rationale: EIM provides the framework for managing and governing information across the enterprise. An EIM program enables data sharing for better decision making and provides County leaders with insight into to the quality of services that they deliver to their citizens.

Timing: Contractor estimates the time required to develop the information management vision and strategy and roadmap to be a 3- to 4- month period that would occur after transition. Contractor would work with the County to determine the business needs and to document the supporting technical requirements. To minimize the County's time investment, while maximizing impact, Contractor would conduct information gathering through a series of focused discussions with stakeholders. This helps Contractor to have an accurate understanding of the current environment as well as the desired future state. At the end of this effort, Contractor would deliver a strategy and roadmap for review and approval by the County.

Risks: None identified.

Dependencies: Developing an effective EIM program is dependent on the active involvement of the business groups as well as the CTO.

Milestones: Key milestones in the planning and implementation of EIM include the following:

- **Milestone 1 – Business Needs Assessment.** A core component of the information gathering phase of the strategy and vision project that focuses on the needs of the business in terms of EIM.
- **Milestone 2 – Current State Assessment.** The second core component of the information gathering phase focuses on documenting the existing technical environment to support EIM
- **Milestone 3 – Desired State Gap Analysis.** The transition step into analysis and planning phase where Contractor documents the gaps between what the County's business needs are and the current technical environment.
- **Milestone 4 – Strawman Vision and Roadmap**. This milestone reflects Contractor draft strategy and roadmap for the County.
- **Milestone 5 – Final Vision and Roadmap.** Once the County reviews and approves, Contractor provides the final strategy and roadmap to guide implementation the of EIM program.

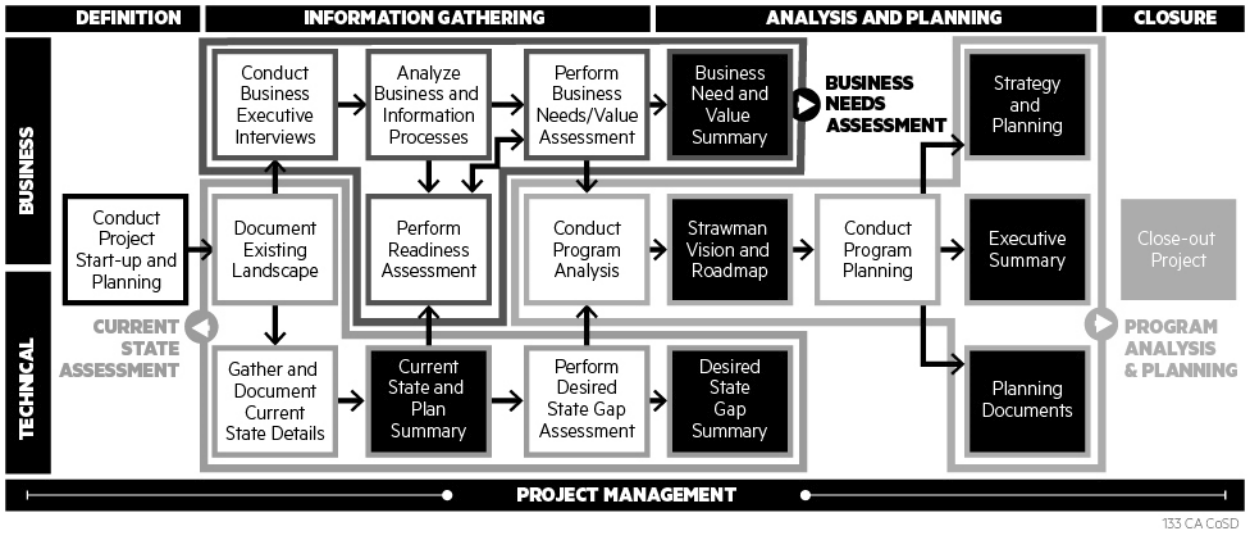
- Deployment plan for resources and use of facilities

For the development of the County's Information Management Strategy, Vision, and the supporting Roadmap, Contractor provides a small team of experienced consultants to work on-site in San Diego with the local support team and key County stakeholders.

- Key methodologies and processes in solution

During the past 40 years, Contractor has developed and documented its IT Solution Architecture (ITSA). This methodology. This methodology would provide the foundation for Contractor's EIM solution. The figure below identifies the detailed steps for both the development of strategy and vision and implementation.

Contractor Global Methods for Information Strategy Master Plan



Contractor uses a collaborative approach to identify and document requirements and gain concurrence for the way forward.

The methodology uses a collaborative approach to align business needs with technology by documenting the current state of technology, process and strategy. Through structured information gathering Contractor documents the desired state and analyze of this information to identify gaps between the current state and the desired state. Contractor uses this information to develop the roadmap to address the gaps. Each step in the framework results in detailed artifacts tailored to the County. Contractor's consultants are trained on the methodology and are experienced in guiding the process, making sure that the County's experience is positive and the results meet their information management needs.

While not included in the proposed initiative, Contractor anticipates that after the County develops its EIM strategy and roadmap, there would be a need to support implementation of EIM. Contractor has a mature methodology for implementation and is prepared to support the County in this phase. This methodology applies proven templates and suggests industry best practices to gather the correct information needed for successful implementation. Contractor would work with Contractor's account team and provide Contractor's expertise to help guide project implementation as identified in the County roadmap. Common implementation projects address information management/quality, master data management, information governance, enterprise data modeling, and development of enterprise standards.

- Automated systems and tools involved in solution

The process for planning and implementing EIM projects relies on standardized templates to gather and document requirements. These result in well-defined deliverables that are guided by an extensive set of artifacts and knowledge libraries. Contractor would use its existing methodologies and associated processes to develop the strategy and plan. As Contractor assesses the current environment and conduct a gap analysis, Contractor documents technology requirements for subsequent implementation projects.

Comprehensive Applications Threat Analysis (CATA) Service Transformation Project

- Description of solution to meet the requirements

Contractor's Comprehensive Applications Threat Analysis (CATA) service uses well-established return on investment (ROI) practices for quality improvement. These practices demonstrate that fixing defects after code implementation can be 30 to 100 times costlier than discovering, avoiding, or reducing the severity of defects early, during requirements analysis, architecture, and design. Conventional software development practices discover and fix only a small fraction of security vulnerabilities later in the application development life cycle; CATA enables achievement of a much higher level of assurance with security and lower rework costs. CATA minimizes security-related rework by helping get it right the first time by identifying security issues in higher layers of abstraction of the application (requirements, architecture, design). This can pervasively improve applications security to complement other efforts to address security issues in source code (static) and run-time behavior (dynamic).

Projects: CATA reviews would be conducted on a subset of the County's applications, selected and prioritized according to factors such as County-provided priority, sensitivity/criticality of data managed by application, impact if the application is compromised (confidentiality, integrity, or availability), significance/scope of application updates (especially new requirements, updated architecture, design, transformation/modernization), any available risk characterizations, and other factors agreed to by Contractor and the County. Likewise, prioritization criteria and decisions would be made for static security code reviews and applications vulnerability assessment and penetration testing. In cases where a CATA review is conducted, and it is deemed appropriate to conduct a follow-on CATA review on the same application (for instance, above the risk prioritization threshold for CATA reviews, and having another major release since prior review), a CATA delta review would be conducted, starting with the CATA baseline analysis initially performed or a prior CATA delta review.

Objectives: the identification of security requirements/controls gaps and vulnerability risks, and recommendations to address (close gaps, lower risks) for each security assessment (CATA, static security code review, vulnerability assessment / penetration test) to improve the security of these applications by a prioritized incorporation of the review recommendations.

Deliverables: A prioritized and vetted list of security findings from each of two CATA phases (Security Requirements Gap Analysis; and Architectural Threat Analysis) with project team commitments to address factored into before and after severities. These can be in the form of summary slides (most common form of deliverable), samples of which are shown below in the Key Methodologies section, or longer written reports at the County's option, which include additional explanatory narrative and background on the specific analysis results

that contributed to the findings. Findings from code review and vulnerability assessment and penetration testing are in the form of written reports describing findings, along with severities and remediation recommendations.

- Key methodologies and processes in solution

CATA is a two-phase activity—Security Requirements Gap Analysis and Architectural Threat Analysis—that includes interviews with Contractor development staff, analysis by Contractor staff and tools, and reporting.

The **Security Requirements Gap Analysis** determines security requirements and control gap for deployment of the application in compliance with applicable regulatory frameworks and industry best practices. The gap analysis would establish security control objectives and lay the groundwork for the threat analysis.

During the Security Requirements Gap Analysis phase, Contractor would identify relevant sources for security requirements derived from applicable regulatory requirements. Contractor then would establish traceability from the County's regulatory or business environment to a prioritized set of security requirements. From the information Contractor gathers through Contractor's proprietary templates and stakeholder interviews, Contractor would determine the plans and commitments for addressing these requirements, with special focus on already-designated technical solutions and already-documented security expectations, and the remaining gaps.

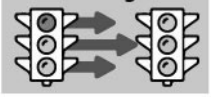
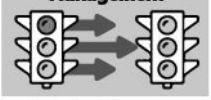
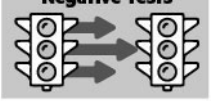
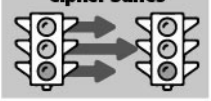
The Security Requirements Gap Analysis is based on:

- Expert system-like templates, with partially encoded expert security knowledge
- Weighted and prioritized input
- Data that is reviewed and calibrated by certified security reviewers
- Efficient, repeatable results
- Requirements traceability from a robust collection of governance sources, including regulations, laws, and best practices.

The end result is a Security Requirements Gap Analysis that would identify important security requirements that may not be met through current plans. It places these at-risk requirements in priority or severity order.

The figure below is a sample of summary level Security Requirements Gap Analysis findings, which would be part of a larger findings slide deck.

Security Requirements Gap Analysis Sample Summary of Findings

Remaining Disconnect and Review Progress	Current Release Impact	Future Roadmap
Lacking Least Privilege 	Daemons (Tomcat/JBoss) exposed to internet run with **full-privilege** accounts, **increasing security risks** and potentially increasing security-related **support cost.** Making customer compliance with GLB, BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** **Modify** Tomcat/JBoss (and other **automated processes**) to **run** as restricted users with **least privilege needed.** It may be necessary to do that for Current Release, depending on Threat Analysis results.
Certificate Lifecycle Management 	Supports **only self-signed certificates,** which **require reliance** on **DNS (proven to be unsecure)** and do **not** allow for **revocation verification,** potentially causing **unauthorized access** to customer **credentials.** Making customer compliance with BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** Add **support for CA signed certificates** and certificate **revocation** thru OCSP or CRL verification.
Missing Security Negative Tests 	**No Security Negative Tests** because QA has no experience with negative testing. Making customer compliance with BS7799, HIPAA, and PCI-DSS difficult.	**Next Release** Train QA team on security test tools (e.g., WebInspect) and **include security negative** tests to test plan.
Non-Configurable Cipher Suites 	The **cipher** and **hash algorithms** are **not configurable.** Thus, **customers** may **not** be able to **follow** their **IT policies** and **cannot disable weak algorithms.** Making customer compliance with HIPAA and PCI-DSS difficult.	**Future Release** Make **cipher and hash algorithms configurable.**

173 CA CoSD

This sample report shows an overall security assessment of Medium Risk from non-supported security requirements.

The **Architectural Threat Analysis** is an architecture-level review of the security properties of the underlying components and interfaces and provides recommendations for mitigating all identified moderate- and high-risk areas.

CATA combines information about the target application and deployment environment with target application security plans. A Contractor security consultant, uses CATA tools and templates that include a requirements traceability questionnaire and database, and an architectural threat analysis heuristic template. These tools add repeatability, semi-automated risk calculations, and serve as an "additional reviewer in the room." Contractor's security consultant then analyzes the resultant data.

In the Architectural Threat Analysis phase, the CATA team acts as an independent party, and would interview the designated Project Security Architect for the specified application or system. Contractor would then review architecture-level documents to gather information regarding architectural interfaces, components, data, and security characteristics, in addition to security mitigations already planned. Contractor has developed a repeatable process that uses a variety of well-established heuristics to identify interfaces and security properties that have the greatest risk of security defects. The Contractor analyst would factor in the risk reduction resulting from the mitigations and controls reportedly applied, and identify areas of residual elevated risk as well as technical control opportunities.

The Architectural Threat Analysis invariably finds unnecessarily elevated security risks that would benefit from additional technical controls. Contractor investigates specific solutions to address the security risks and provides recommendations based on best fit for the County's organization and mission. This task does not include implementation of the solutions. Architectural Threat Analysis can preempt building security flaws into applications based on the following elements:

- Expert system-like artifacts, encoded with first-order expert security knowledge
- Weighted and prioritized input
- Data that is reviewed and calibrated by certified security reviewers

- Efficient, repeatable results.

The figure below is a sample of summary level Architectural Threat Analysis findings (part of a larger findings slide deck).

Sample Architectural Threat Analysis Report

Security Risk Area and Review Progress	Past Behavior	Fix
Least Privilledge	All **process** daemons **running as root** gaining **full access** to the box and **defects can lead to unauthorized** code running as **root**	Create **restricted user** account and use it to **run** the process **daemons**
Support for Third-Party Certificates	Using **self-signed** certificates **hinders** customer **validation, exposing** customer and servers to **man-in-the-middle attacks.**	**Replaced self-signed certificates and provided** means for **validating the certificates** correctly
Full Privilledge Database Account	**Web application using** an admin **root account** was **unnecessarily** risking to **expose database data**	**Replaced admin** account by **restricted account**
Duplication of Validation Routines	Validation routines were disperse in the code raising the risk of missing bug fixes	**Integrate** in the project a **well-documented** validation **library**
World-Writable Directory	Web application **configuration files** were **world-writable exposing** them to an external **attacker** to be able to **modify important application characteristics**	Included **file system checks** in build **scripts**
Exposed Passwords	Web application and CC service would **leave credit card** information in **clear text** after **freeing memory**	**Wipe memory buffer** before freeing memory

174 CA CdSD

The Architectural Threat Analysis prevents security risks from being introduced into application code.

Missing or incomplete security requirements, architectural threats, and/or previously investigated remediation may be identified during the analysis. Contractor would report these findings based on their severity: High (Red), Moderate (Yellow), and Low (Green). Severities can be modified if required to match specific regulatory frameworks.

Findings would include a high-level executive summary, slide tables of individual prioritized findings with remediation recommendations, and if a written report is required, a technical discussion section.

While CATA is highly effective for proactively identifying and mitigating potential security risks in the targeted applications, Contractor recommends combining CATA with secure code analysis by a security expert using the Fortify tool or with hybrid combinations such as Contractor's human expert security code reviews, in addition to Contractor's applications vulnerability assessment and penetration testing. This would result in identifying vulnerabilities through both static and dynamic security analysis, as these highly complement CATA. Static security analysis identifies issues in source code, and dynamic security analysis identifies vulnerabilities in run-time behavior, while CATA identifies security issues in requirements, architecture, and high-level design.

CATA – Complementary Security Services: CATA is a high-level service focused on the requirements and architectural level. Problem areas identified through CATA can often be addressed through other Contractor security service offerings. The following additional services help assess whether the security designed in early stages is also implemented correctly:

- **Secure Code Analysis** – Provides validation that the application, once it has been designed correctly, is implemented as designed. This may be a combination of human expert security code review and automated static scanning, such as with HPE Fortify.

- **Applications Vulnerability Assessment** – Provides a further layer of validation that once the application is implemented as designed, known attack vectors do not "break" it. Vulnerability assessment can be performed not only prior to deployment, but also throughout the production lifetime of the application. The assessment can catch some emerging or "zero day" problems with applications that have already been deployed to the field.
- **Penetration Testing** – Penetrates beyond vulnerability assessment to test vulnerabilities discovered in vulnerability assessment for exploitability.

- Automated systems and tools involved in solution

HPE Fortify on Demand, CATA tools and templates, referenced above. Note that HPE Fortify is distinct from CATA, which analyzes analyses security requirements, architecture, and high-level design, and is human methodology, whereas Fortify is a product/tool to scan code statically (for instance Fortify SCA) and dynamically (WebInspect). These tools are highly complementary, and when used in combination with human expert and hybrid Secure Code Analysis and application vulnerability assessment and penetration testing, they cover security across all major aspects of the SDLC.

10. CONTRACTOR TOOLS

Following is a list of the tools used in Contractor's solution to provide services to the County.

RESOURCE / TOOL NAME	INFORMATION
Enterprise System List (ESL)	Type: Software Manufacturer: HPES Purpose/Use: ESL (Enterprise System List) is a Delivery-focused Configuration Management System for managing System/Application Configuration Items, Services/Contracts and Customer/Account Information. Other Information: Supported Services: Configuration Management Services
Asset Manager	Type: Software Manufacturer: HPE Purpose/Use: Tracks End-User and network assets Other Information: Supported Services: Configuration Management Services, End User Services, Domain Name Management Services Supported Services: Cross Functional
Discovery and Dependency Mapping Inventory (DDMI)	Type: Software Manufacturer: HPE Purpose/Use: discovers and reports assets found on the network; integrates with Asset Manager. Other Information: Supported Services: Cross Functional
Service Manager (HPSM)	Type: Software Manufacturer: HPE Purpose/Use: Used by the Service Desk and all support staff for ticketing of Incidents, Problems and Changes. Other Information: Supported Services: Service Delivery Management, Incident Management, Problem Management Services, Change Management Services, Release Management Services, Service Desk Services, End User Services, Core Software Services, County Retained Assets Services, Catalog Services, Network Printer Services, Configuration Management Services
End User Access (EUA)	Type: Software Manufacturer: HPES Purpose/Use: Service Portal Other Information: While the core software and interfaces are standardized and centrally controlled to interact with the rest of the cross functional tools, the Service Portal is separately instantiated and customized for each client for whom it is deployed.

RESOURCE / TOOL NAME	INFORMATION
	Supported Services: Project Management Services, Reporting Management Services, County Retained Asset Services, Catalog Services, Application Maintenance and Operations Services
Aries/Aldea	Type: Software Manufacturer: HPES Purpose/Use: Tool used by Contractor internally to request resources (e.g., staffing assignments, workload placement) from the broader Contractor community Other Information: Supported Services: Cross Functional
RevGen	Type: Software Manufacturer: SAP Ariba Purpose/Use: Procurement of products and services Other Information: Supported Services: Cross Functional
Enabling Delivery and Global Excellence (EDGE)	Type: Knowledge Repository Manufacturer: HPES Purpose/Use: EDGE is a holistic environment that includes all the information needed to enable Enterprise Services (ES) to deliver and excel in the global marketplace. EDGE supports all individuals in each of the ES business units by providing process artifacts that can be leveraged and used as part of their day-to-day work. Other Information: Supported Services: Architecture Services, Business Analyst Services, Project Management Services
Enterprise Architect	Type: Software Manufacturer: Sparx Systems Purpose/Use: Enterprise Architect provides full life cycle modeling for: Business and IT systems Software and Systems Engineering Real-time and embedded development Other Information: Supported Services: Architecture Services
ProVision	Type: Software Manufacturer: OpenText Purpose/Use: ProVision is Contractor's standard modeling tool, to be used for Business Process, Enterprise Architecture and IT solution modeling. It enables business & IT teams to visually create models, describing business process, process interactions and detailed workflow Other Information: Supported Services: Architecture Services, Business Analyst Services*

RESOURCE / TOOL NAME	INFORMATION
Disaster Recovery Subscription Services	Type: Disaster Recovery Subscription Services Manufacturer: various Purpose/Use: DR subscription services for all leveraged hardware and software used to provide: Server services, Storage services, Network services, Security services and Backup services Other Information: Note that the Centera and the dedicated firewalls located in the DR site are not considered to be part of this list, since they are dedicated to the County. Supported Services: Cross Functional
ArcSight Security Information and Event Management (SIEM)	Type: Software/appliance Manufacturer: HPE Purpose/Use: Event logging and monitoring Other Information: Supported Services: Security Services
Global Delivery Capacity & Performance Management (GDCPM)	Type: Software Manufacturer: HPES (based on SAS and other underlying tools) Purpose/Use: Collects, aggregates and analyzes capacity and performance data from various disparate sources for reporting and analysis Other Information: Supported Services: Capacity Planning and Performance Management Services
System Center Configuration Manager (SCCM)	Type: Software Manufacturer: Microsoft Purpose/Use: Hardware discovery and software distribution to End-User devices Other Information: Security patching of OS and distribution of desktop software Supported Services: End User Services, Core Software Services, County Retained Assets Services, Catalog Services, Application Maintenance and Operations Services, Initiatives: User Data Services
Leveraged Internet Service (LIS) firewalls in the Tulsa and Colorado Springs data centers	Type: Hardware Manufacturer: Checkpoint Purpose/Use: Internet access/security Other Information: In the future these are slated to be replaced by Fortinet firewalls Supported Services: Network Services
AT&T Commonly Shared Network	Type: equipment, tools, software, systems and other materials Manufacturer: Various Purpose/Use: For clarity, the AT&T Commonly Shared Network means (i) the public or shared networks of AT&T, its Affiliates and their subcontractors, and the equipment, tools, technologies, systems, software, and other materials that are components thereof; (ii) equipment, tools, technologies, systems, software and other materials used by AT&T, its Affiliates and their subcontractors in shared network management and back office environments including ,

RESOURCE / TOOL NAME	INFORMATION
	without limitation, TIRKs, iGEMS, BusinessDirect, Billing Edge, the AT&T Global Network Client and AT&T Connect and any other items listed above in this Exhibit; and (iii) all modifications, upgrades, derivative works, enhancements, improvements and extensions of any of the foregoing. Other Information: Supported Services: Network Services
SIMS (Security Information Management System)	Type: Software Manufacturer: AT&T Purpose/Use: Security event correlation Other Information: Supported Services: Network Services
SDNOM (Software Defined Network Order Management)	Type: Software Manufacturer: AT&T Purpose/Use: Circuit Ordering Other Information: Supported Services: Network Services
Nectar Unified Communication Management Platform	Type: Software Manufacturer: Nectar Purpose/Use: Voice Network Performance Management Other Information: Supported Services: Network Services
MDM-Airwatch SaaS Console (Mobile Device Management)	Type: Software Manufacturer: AT&T Purpose/Use: Mobile device management Other Information: Offers a centralized dashboard to enforce policies, set restrictions, and secure devices while in use, lost, or stolen. Supported Services: End User Services, County Retained Assets Services, Mobility Infrastructure Services
SORD (Service Order Retrieval and Distribution)	Type: Software Manufacturer: AT&T Purpose/Use: Service order entry Other Information: Supported Services: Network Services
Telegence	Type: Software Manufacturer: AT&T Purpose/Use: Billing Other Information: Supported Services: Network Services
BOSS (Billing and Ordering Support System)	Type: Software Manufacturer: AT&T Purpose/Use: Product billing, tracking and reporting Other Information: Supported Services: Network Services

RESOURCE / TOOL NAME	INFORMATION
DPSS (Data Products and Services System)	Type: Software Manufacturer: AT&T Purpose/Use: Data product and services tracking Other Information: Supported Services: Network Services
BusinessDirect/eBill	Type: Software Manufacturer: AT&T Purpose/Use: Account management Other Information: Supported Services: Network Services
Exchange Plus	Type: Software Manufacturer: AT&T Purpose/Use: Carrier resource tracking Other Information: Supported Services: Network Services
ICES (Integrated Customer Enterprise System) ServiceCenter/AssetCenter	Type: Software Manufacturer: AT&T Purpose/Use: Asset Inventory Other Information: Supported Services: Network Services
SAINT	Type: Software Manufacturer: AT&T Purpose/Use: Security scanning and testing Other Information: Supported Services: Network Services
Nmap	Type: Software Manufacturer: Nmap Purpose/Use: Network scanning and mapping Other Information: Supported Services: Network Services
WFA (Work Force Administration)	Type: Software Manufacturer: Telcordia Purpose/Use: Trouble ticketing and work flow Other Information: Supported Services: Network Services
TIRKS (Trunks Integrated Record Keeping System)	Type: Software Manufacturer: Telecordia Purpose/Use: Circuit design Other Information: Supported Services: Network Services
AOTS-TM (AT&T One Ticketing System – Trouble Management)	Type: Software Manufacturer: AT&T/Remedy Purpose/Use: trouble ticketing Other Information:

RESOURCE / TOOL NAME	INFORMATION
	Supported Services: Network Services
NMA (Network Monitoring and Analysis)	Type: Software Manufacturer: Telecordia Purpose/Use: Network monitoring Other Information: Supported Services: Network Services
Avaya Site Administration	Type: Software Manufacturer: Avaya Purpose/Use: Voice system administration Other Information: Supported Services: Network Services
Server Automation	Type: Software Manufacturer: HPE Purpose/Use: Distributing operating system and layered product patches and upgrades Other Information: The core mesh is a shared resource; distribution satellite servers within the County's network zones are dedicated to the County Supported Services: Managed Private Cloud
Operations Manager (HPOM)	Type: Software Manufacturer: HPE Purpose/Use: Monitoring and alerting for various data center components, such as servers, domain controllers, databases, etc. Other Information: Supported Services: Managed Private Cloud, Application Maintenance and Operations Services
Microsoft Office 365 Government Community Cloud	Type: Software as a Service Manufacturer: Microsoft Purpose/Use: E-Mail (Exchange Online), Collaboration (SharePoint Online, Skype for Business), Cloud File Management (OneDrive for Business) Other Information: Supported Services: Data Center Services
E2E Complete	Supported Services: Transition Schedule and Tasks Type: Software Manufacturer: BinaryTree Purpose/Use: Automation tool for migration of mail services from Exchange to the Microsoft Office 365 Cloud Other Information: Supported Services: Unified Communications Infrastructure Services
Helion Virtual Private Cloud for US Public Sector	Type: Infrastructure as a Service Manufacturer: HPE Purpose/Use: Virtual Private Cloud (VPC) for Windows and Linux environments. VPC is a Government Community Cloud currently used to run the County's Beach and Water Quality website.

RESOURCE / TOOL NAME	INFORMATION
	Other Information: Data Center Services
Watchdog	Type: Software Manufacturer: HPES Purpose/Use: Internally developed utility that monitors/removes privileged access implemented via non-approved methods Other Information: Supported Services: Security Services
StarTeam	Type: Software Manufacturer: Microfocus/Borland Purpose/Use: Software Change and Configuration Management Other Information: This tool may also be used in Business Analysis and Applications M&O Supported Services: Applications M&O
Together	Type: Software Manufacturer: Microfocus/Borland Purpose/Use: Together enables software to be designed using industry-standard UML notation and conventions. With a large number of built-in utilities to manage the software design process, validate designs and generate code, together helps maximize the efficiency and accuracy of the software development process Other Information: This tool may also be used in Business Analysis and Applications M&O Supported Services: Business Analyst Services
Agile Manager	Type: Software Manufacturer: HPE Purpose/Use: Agile project management is a SaaS (software-as-a-service) solution that helps teams to organize, plan, and execute Agile projects. Other Information: This tool may also be used in Business Analysis and Applications M&O Other Information: Supported Services: Applications M&O
Team Foundation Server	Type: Software Manufacturer: Microsoft Purpose/Use: Microsoft Team Foundation Server (TFS) is a set of tools and technologies that enable a team to collaborate and coordinate the development and build efforts for a .NET software product or completing a .NET software project. Other Information: This tool may also be used in Business Analysis and Applications M&O Supported Services: Configuration Management Services
MEGA	Type: Software Manufacturer: Mega

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: to help enterprise architects and business stakeholders get a digital representation of their organization and its strategy, goals, business processes, and resources. Other Information: Supported Services: Architecture Services
Project and Portfolio Management (PPM)	Type: Software Manufacturer: HPE Purpose/Use: Project Management Integration, prioritization, demand management Other Information: SAAS Solution Supported Services: Architecture Services, Project Management Services, Business Analyst Services, Applications Maintenance and Operations Services
Apps (Applications) Manager	Type: Software Manufacturer: HPES Purpose/Use: to track and report on Portfolio Application information. Other Information: Supported Services: Architecture Services, Configuration Management Services
MS SharePoint	Type: Software Manufacturer: Microsoft Purpose/Use: Collaboration, Integration, Reporting and Workflow Other Information: Supported Services: Project Management, Reporting Management
myRequests	Type: Software Manufacturer: HPES Purpose/Use: Requests Management, Collaboration, Integration and Workflow Other Information: Supported Services: Project Management, Reporting Management
DocVault	Type: Software Manufacturer: HPES Purpose/Use: Collaboration and Document Storage Other Information: Custom Documentum and SharePoint Integration for storage of documentation Supported Services: Project Management, Reporting Management
Application Lifecycle Management (ALM)	Type: Software Manufacturer: HPE Purpose/Use: Quality Management, Testing Management and Measurement, functional testing. Manage test cases and test scripts and track test results Other Information: SAAS Solution Supported Services: Integration and Testing Services, Applications Development Services

RESOURCE / TOOL NAME	INFORMATION
Requirements Ambiguity Checker	Type: Software Manufacturer: HPE Purpose/Use: Requirements Validation Other Information: Supported Services: Integration and Testing Services
Performance Center	Type: Software Manufacturer: HPE Purpose/Use: Performance Testing Other Information: Supported Services: Integration and Testing Services
Unified Functional Tester	Type: Software Manufacturer: HPE Purpose/Use: Regression Testing Other Information: Supported Services: Integration and Testing Services
WebLogic Server 11gR1 Generic and Coherence	Type: Software Manufacturer: Oracle Purpose/Use: Middleware Other Information: Supported Services: Identity and Access Management Services
Identity Manager	Type: Software Manufacturer: Oracle Purpose/Use: Manage End-User access privileges Other Information: Supported Services: Identity and Access Management Services, Initiative: Identity Federated Services
Access Manager	Type: Software Manufacturer: Oracle Purpose/Use: Provides adaptive authentication, federated single sign-on (SSO), risk analysis, and fine-grained authorization extended to mobile clients and mobile applications. Other Information: Supported Services: Identity and Access Management Services, Initiative: Identity Federated Services
Fusion Middleware Repository Creation Utility 11g	Type: Software Manufacturer: Oracle Purpose/Use: Code Repository Other Information: Using SVN Supported Services: Identity and Access Management Services
Enterprise Content Management 11g	Type: Software Manufacturer: Oracle Purpose/Use: Content Management Other Information: Supported Services: Identity and Access Management Services

RESOURCE / TOOL NAME	INFORMATION
SQL Server Business Intelligence	Type: Software Manufacturer: Microsoft Purpose/Use: Creating SQL Queues and Reports Other Information: Supported Services: Reporting Management Services
MindMeister	Type: Software Manufacturer: Purpose/Use: Online mind mapping tool that enables users to capture, develop, and share ideas visually Other Information: Supported Services: Business Analyst Services*
Active Directory and Group Policy	Type: Software Manufacturer: Microsoft Purpose/Use: Used to manage the database of resources on the network Other Information: Microsoft environment printer management tools Supported Services: End User Services, Network Printer Services, Initiative: Identity Federated Services
Office Configuration Analyzer Tool (OffCAT)	Type: Software Manufacturer: Microsoft Purpose/Use: Provides a detailed report on installed Office programs and Highlights known problems Other Information: Supported Services: End User Services
Diagnostic Toolset	Type: Software Manufacturer: HPE Purpose/Use: Hardware diagnostics includes hard drive scanning repair, memory testing Other Information: Supported for Win7 and Win10 Supported Services: End User Services
Endpoint Protection / Encryption	Type: Software Manufacturer: Symantec Purpose/Use: Full disk and removable media encryption management. Anti-virus and anti-malware solution Other Information: Supported Services: End User Services, Core Software Services, Security Services
LogMeIn Rescue (LMI)	Type: Software Manufacturer: LogMeIn Purpose/Use: Provides secure remote control into End-User's device, to investigate and resolve issues Other Information: Supported Services: End User Services

RESOURCE / TOOL NAME	INFORMATION
Forcepoint Data Loss Prevention	Type: Software Manufacturer: WebSense Purpose/Use: Data loss protection on workstations Other Information: Supported Services: Core Software Services
Managed PKI	Type: Software Manufacturer: Symantec Purpose/Use: Device certificates for authentication Other Information: Supported Services: Core Software Services
Nessus	Type: Software Manufacturer: Tenable Network Security Purpose/Use: Vulnerability scans of workstations Other Information: Supported Services: Core Software Services, Security Services
Metasploit	Type: Software Manufacturer: Metasploit Purpose/Use: Validates that security of the core software configuration is acceptable prior to addition of new components to the configuration Other Information: Penetration Testing Supported Services: Core Software Services, Security Services
Expert Systems	Type: Software Manufacturer: Avaya Purpose/Use: Avaya maintenance services include Avaya Expert Systems and Secure Access Link (SAL). Avaya Expert Systems provides the County with Core Voice Services, a maintenance database of more than 30,000 artificial intelligence algorithms (AIAs) with scripted automation. These scripts automatically correct many known system- and software-related issues. Avaya SAL is a centralized consolidation point for all Avaya core systems for health and alarm monitoring, secure remote access using secure outbound-only HTTPS, and an integration point for Avaya Expert Systems. Other Information: Supported Services: Mobile Device Support Services, Voice Services, Initiative: Voice Services Transformation
Unified Communication Management Platform (UCMP)	Type: Software Manufacturer: Nectar Services Corp Purpose/Use: provides multivendor management services including application dependency, tree visual alerting, and vendor knowledge modules Other Information: Supported Services: Mobile Device Support Services, Voice Services, Initiative: Voice Services Transformation

RESOURCE / TOOL NAME	INFORMATION
CA eHealth	Type: Software Manufacturer: CA Technologies Purpose/Use: Performs capacity, performance, and trend analytics for circuits Other Information: Supported Services: Data Network Services, Video Conferencing Services, Wireless Network Access Services, Third-Party Network Access Services, IP Address Management Services
CA Spectrum	Type: Software Manufacturer: CA Technologies Purpose/Use: Monitors all network equipment—routers, switches, wireless access point (WAP) controllers, and WAPs—and provides alerts/alarms based on predefined parameters Other Information: Supported Services: Data Network Services, Remote Access Services, Video Conferencing Services, Wireless Network Access Services, Third-Party Network Access Services, IP Address Management Services, Initiatives: IT Application Portfolio Management Services
Cascade Shark	Type: Software Manufacturer: Riverbed Purpose/Use: Performs NetFlow data capture for subsequent troubleshooting and in-depth packet analysis by Cascade Pilot Other Information: Supported Services: Data Network Services, Application Maintenance and Operations Services*, Initiatives: IT Application Portfolio Management Services
Cascade Pilot	Type: Software Manufacturer: Riverbed Purpose/Use: Performs in-depth network packet analysis Other Information: Supported Services: Data Network Services
SMARTnet Total Care (SNTC)	Type: Software Manufacturer: Cisco Purpose/Use: Discovers and reports on all Cisco equipment and maintains the database of all Cisco equipment. Automates the process of gathering data for direct vendor support in the event of a problem. Other Information: Supported Services: Data Network Services, Initiatives: IT Application Portfolio Management Services
AirWave	Type: Software Manufacturer: Aruba Purpose/Use: Provides inventory and control of wireless access points and controllers Other Information: Supported Services: Data Network Services, Wireless Network Access Services

RESOURCE / TOOL NAME	INFORMATION
Prime Infrastructure	Type: Software Manufacturer: Cisco Purpose/Use: Provides Cisco equipment configuration management and control; backs up equipment configurations and manages licenses Other Information: Supported Services: Data Network Services, Wireless Network Access Services, Initiatives: IT Application Portfolio Management Services
Juniper JSA3800	Type: Software Manufacturer: Juniper Networks Purpose/Use: Collects logging information about all remote access connections and supports the routine review of the logs Other Information: Supported Services: Remote Access Services
Wireless Control System (WCS)	Type: Software Manufacturer: Cisco Purpose/Use: to measure and take action to maximize performance of the network, as well as to provide ongoing reporting. Other Information: Supported Services: Wireless Network Access Services
Luna Control Center	Type: Software Manufacturer: Akamai Purpose/Use: to perform the essential activities of external DNS support Other Information: Supported Services: External DNS Management Services
PAM Adonis and Proteus systems	Type: Software Manufacturer: BlueCat Networks Purpose/Use: to collectively fulfill all of the IPAM requirements and support adherence to the service level requirements Other Information: Supported Services: IP Address Management Services
MS Project	Type: Software Manufacturer: Microsoft Purpose/Use: planning and tracking Other Information: Supported Services: Project Management Services, New Site Installation Services
MS Excel	Type: Software Manufacturer: Microsoft Purpose/Use: planning and tracking Other Information: Supported Services: Project Management Services, New Site Installation Services

RESOURCE / TOOL NAME	INFORMATION
MS PowerPoint	Type: Software Manufacturer: Microsoft Purpose/Use: planning and tracking Other Information: Supported Services: Project Management Services, New Site Installation Services
Exchange Online Protection	Type: Software Manufacturer: Microsoft Purpose/Use: Antivirus protections, Antispam filters, Policy enforcement, Graymail detection, safe-unsubscribe, Email based threats (phishing, targeted attacks), Outbreak filters, Data Loss Prevention, Email Encryption Other Information: Supported Services: Security Services
Controlled Compliance Suite (CCS)	Type: Software Manufacturer: Symantec Purpose/Use: Policy compliance for servers Other Information: Supported Services: Security Services
Enterprise Reporter	Type: Software Manufacturer: Dell Purpose/Use: Active Directory Reporting Other Information: Supported Services: Security Services
Recovery Manager AD	Type: Software Manufacturer: Dell Purpose/Use: Restore deleted or corrupted objects and domain or forest Other Information: Supported Services: Security Services
Cloud Service Automation	Type: Software Manufacturer: HPE Purpose/Use: Automation of cloud management and provisioning Other Information: Supported Services: Managed Private Cloud
Helion Managed Cloud Broker	Type: Software Manufacturer: HPE Purpose/Use: This tool is extendable to remote virtual environments and can integrate with public cloud vendors such as Amazon Web Services and Microsoft Azure Other Information: Supported Services: Managed Private Cloud
Operations Orchestration Server (OO)	Type: Software Manufacturer: HPE Purpose/Use: Process workflow automation Other Information:

RESOURCE / TOOL NAME	INFORMATION
	Supported Services: Managed Private Cloud
Operations Orchestration Remote Access Server	Type: Software Manufacturer: HPE Purpose/Use: Remote access to OO Other Information: Supported Services: Managed Private Cloud
v-Center	Type: Software Manufacturer: VMware Purpose/Use: Server virtualization management Other Information: Supported Services: Managed Private Cloud
Infoscale	Type: Software Manufacturer: Veritas Purpose/Use: Filesystem management and clustering in specific Solaris environments Other Information: Supported Services: Managed Private Cloud*
Storage Foundation	Type: Software Manufacturer: Symantec Purpose/Use: Filesystem management and clustering in specific Solaris environments Other Information: Supported Services: Managed Private Cloud*
SiteScope	Type: Software Manufacturer: HPE Purpose/Use: for monitoring application thresholds and events Other Information: Supported Services: Managed Private Cloud
Codar	Type: Software Manufacturer: HPE Purpose/Use: For version-controlled, one-click deployments, rollbacks and promotions Other Information: Supported Services: Development and Test Services, Application Development Services
3PAR System Utilities	Manufacturer: 3PAR Purpose/Use: 3PAR array-based replication allows background replication of storage from one array to another. 3PAR Storage Peer Motion is used to migrate storage data volumes without any interruption in accessing the data. Other Information: Supported Services: Storage Services, Storage Architecture Type: Software

RESOURCE / TOOL NAME	INFORMATION
BUR Dashboard	Type: Software Manufacturer: HPES Purpose/Use: This notifies BUR admins and End-Users of both successful and missed backups. It identifies for the BUR admins which nodes to work and automates BUR jobs Other Information: Supported Services: Backup and Recovery Services
Print Server	Type: Software Manufacturer: BARR Systems Purpose/Use: To automate and control print and document output Other Information: Supported Services: Managed Print Services
Symantec Management Console	Type: Software Manufacturer: Symantec Purpose/Use: to provision and revoke certificates and configure applications to use those certificates, reporting, and administrative End-User management services Other Information: Supported Services: Public Key Infrastructure Services
Applications Performance Management (APM)	Type: Software Manufacturer: HPE Purpose/Use: Provides a 360-degree view that verifies the performance of desktop, web, and mobile apps for on premise, cloud, or hybrid environments Other Information: Supported Services: Application Maintenance and Operations Services*
Toad	Type: Software Manufacturer: Dell Purpose/Use: For Oracle software Other Information: Supported Services: Application Development Services
PST Capture	Type: Software Manufacturer: Microsoft Purpose/Use: For searching and harvesting PST files Other Information: Supported Services: Transition Schedule and Tasks
DoubleTake	Type: Software Manufacturer: Vision Solutions Purpose/Use: a migration tool that performs a complete server copy from the source server onto the target server. Other Information: Supported Services: Consolidated and Single Data Center

RESOURCE / TOOL NAME	INFORMATION
PlateSpin	Type: Software Manufacturer: NetIQ Purpose/Use: Similar to DoubleTake, PlateSpin performs a complete server copy from the source server to the target server, if needed. It allows source servers to be copied as an image that can be transported using an approved portable storage device Other Information: Supported Services: Consolidated and Single Data Center
Panorama	Type: Software Manufacturer: Palo Alto Networks Purpose/Use: Provides a central repository for logging, inventory of the Palo Alto components, licensing management, software image management, and analysis Other Information: Supported Services: Initiatives: IT Application Portfolio Management Services
E911 Manager	Type: Software Manufacturer: Unknown Purpose/Use: Automates the E911 management process by connecting with the County's Geo-Redundant Avaya Communications Manager to the AT&T MPLS network to track and update VoIP, digital, and analog phone moves, adds, and changes. Other Information: Supported Services: Initiative: Voice Services Transformation, Initiative: E911
E911 Anywhere	Type: Software Manufacturer: Unknown Purpose/Use: A cloud-based 911 call routing service that can connect a 911 call to more than 6,000 Public Safety Answering Points (PSAPs) in the U.S. and Canada. Other Information: Supported Services: Initiative: Voice Services Transformation, Initiative: E911
SPM	Type: Software Manufacturer: Unknown Purpose/Use: Unknown Other Information: Supported Services: Initiative: Storage Architecture
ControlPoint	Type: Software Manufacturer: HPE Purpose/Use: Analyzing unstructured data for cleaning up and archive Other Information: Supported Services: Initiative: Storage Architecture
SDM	Type: Software Manufacturer: HPE

RESOURCE / TOOL NAME	INFORMATION
	Purpose/Use: To reduce the data footprint of structured data Other Information: Supported Services: Initiative: Storage Architecture
OneView	Type: Software Manufacturer: HPE Purpose/Use: Common software-defined convergence platform Other Information: Supported Services: Initiative: Storage Architecture
Federation Manager Identity Federation (OIF)	Type: Software Manufacturer: Oracle Purpose/Use: Provides secure identity information exchange between external/internal partners. OIF provides account management for partner identities and integrations. OIF integrates with a wide variety of data stores, End-User directories, authentication providers, and applications. Other Information: Supported Services: Initiative: Identity Federated Services
Virtual Directory, Unified Directory	Type: Software Manufacturer: Oracle Purpose/Use: Internet and industry-standard Lightweight Directory Access Protocol (LDAP) and eXtensible Markup Language (XML) views of existing enterprise identity information without synchronizing or moving data from its native locations. Other Information: Supported Services: Initiative: Identity Federated Services
Active Directory Federated Services (ADFS)	Type: Software Manufacturer: Microsoft Purpose/Use: Provide users with SSO access to systems and applications located across organizational boundaries. Other Information: Supported Services: Initiative: Identity Federated Services
Fortify on Demand	Type: Software Manufacturer: HPE Purpose/Use: To scan code statically Other Information: Supported Services: Other Proposed Initiative: Comprehensive Applications Threat Analysis (CATA) Service
Netcool	Type: Software Manufacturer: IBM Purpose/Use: Monitoring data center network devices Other Information: Supported Services: Network Services

RESOURCE / TOOL NAME	INFORMATION
Network Node Management Interface (NNMi)	Type: Software Manufacturer: HPE Purpose/Use: Monitoring performance/capacity of data center circuits and devices Other Information: Supported Services: Network Services
Wireshark	Type: Software Manufacturer: Wireshard Purpose/Use: such as for deep packet capture analysis Other Information: Supported Services: Network Services
Bluejeans	Type: Software Manufacturer: Bluejeans Purpose/Use: portal access to evaluate End-User and conference usage and detail Other Information: Supported Services: Video Conferencing Services
Enterprise Manager	Type: Software Manufacturer: Oracle Purpose/Use: to provide performance metrics, historical data, trending & reporting. Other Information: Supported Services: Supported Services: Video Conferencing Services
PVCS	Type: Software Manufacturer: Serena Purpose/Use: Archived project documents and application code Other Information: Supported Services: Supported Services: Applications Services, Project Management Services
AssetEdge Lease Manager	Type: Software Manufacturer: HPE Financial Services Purpose/Use: Lease tracking Other Information: Supported Services: Asset Management Services
PKI	Type: Software Manufacturer: Microsoft Purpose/Use: Certificate authentication Other Information: Supported Services: Security Services
Pretty Good Privacy (PGP)	Type: Software Manufacturer: Symantec Purpose/Use: File encryption Other Information: Supported Services: Security Services

RESOURCE / TOOL NAME	INFORMATION
StoreServ Management Console	Type: Software Manufacturer: HPE Purpose/Use: 3PAR management and reporting console for converged management of both File and Block on HPE 3PAR StoreServ Storage systems. Other Information: Supported Services: Storage Services, Storage Architecture
3PAR Command Line interface (3PAR CLI)	Type: Software Manufacturer: HPE Purpose/Use: To monitor, manage, and configure 3PAR storage Systems. Other Information: Supported Services: Storage Services, Storage Architecture

*Tool is listed as an option for use with this Service

11. COUNTY APPLICATIONS BY PA-ID

PAID	NAME
PA1002	AIS Master Mailing List
PA1005	AAB Labels
PA1008	ACAP/ACVV Values, Rates, Apportion
PA1014	Accounts Receivable and Trust
PA1017	ACRC Roll Corrections Process
PA1018	ACST/TC Auditor Secured Tax Billing
PA1019	ACTI Tax Rate Area Index
PA1020	ACUS Auditor Unsecured Prpty Tax Billing
PA1024	Agricultural Preserves
PA1044	ASAD Secured Prpty Assess Info System
PA1045	ASAS Secured Prpty Assess Ownership&Valu
PA1046	ASPA Supplemental Property System
PA1047	ASRC Roll Corrections Process
PA1048	Assessment Appeals Board System
PA1049	ARCC Intranet Applications
PA1050	ARCC Internet Applications
PA1054	Audit Assignment Tracking
PA1058	AutoCAD
PA1073	CDS Online
PA1074	CDS Batch
PA1077	Ballot Enclosure Scanning System
PA1136	Chameleon
PA1158	Community Enhancement / Neighborhood Reinvestment Program (AC Grant)
PA1159	iVOS
PA1160	Comparable Sales System
PA1162	Computer Assisted Mass Appraisal (CAMA)
PA1174	County Law
PA1179	Criminal Case Tracking-JURIS
PA1187	Cut Log Tracking

PAID	NAME
PA1188	County Intranet Site
PA1196	CME Web
PA1202	DHR Internet Class/Comp info.
PA1247	Field Survey Notes Index
PA1270	Geo-Coding System
PA1308	TTC Sonant IVR, ACD and Phone Payment System
PA1310	Homeowner Exemptions - AS/400
PA1313	IBM - Probation Records
PA1314	IDX Managed Care Application
PA1324	Interest Apportionment
PA1376	Traffic/Minor Offense Mainframe
PA1389	MPR Online
PA1409	Officer Notification System
PA1433	PAR File Online
PA1438	Precinct Activity Tracking System
PA1451	Performance Reports
PA1516	Prop 60/90/110
PA1517	Prop 8
PA1523	TTC Tax Sale Database
PA1564	Records Index
PA1566	Redemption (Prior Year/Secured/Defaulted) Taxes
PA1568	DPW Referrals System
PA1580	Restraining Order System
PA1588	RSVP Volunteer Reporter
PA1595	Sale of Data
PA1603	Section 11 Properties
PA1609	Sheriff ID
PA1610	Sheriff Licensing
PA1611	Sheriff Registrants
PA1643	Supplemental Online
PA1659	Timeshare Ownership Tracking
PA1665	Criminal History Tracking System

PAID	NAME
PA1680	TTC TRDS Defaulted Secured Data Mgmt (Mainframe)
PA1682	TTC TRST Tax Collector Secured Tax Collect (Mainframe)
PA1683	TTC TRTC Carryover (Mainframe)
PA1684	TTC TRTH Secured Tax History Info System (Mainframe)
PA1742	TTC TRRT Unsecured Tax Refund Mgmt System (Mainframe)
PA1745	TTC TRUS Unsecured Property Tax System (Mainframe)
PA1755	Volunteer Tracking System Polinsky
PA1759	Want/Warrant System
PA1766	Weather Monitoring and Flood Warning System
PA1782	Adoptions Assistance Program
PA1785	Animal Control - Lost and Found
PA1788	Autocad
PA1789	AutoLISP Files
PA1802	TTC TRCC Cortac (Mainframe)
PA1809	CWS/CMS Data Mart
PA1813	TTC Tax Sale Maps and Images (Web)
PA1814	DHR Internet Web Page
PA1820	EMISSIONS INVENTORY (EASIER)
PA1846	Natality Extract for Dr. Dobkins, UCSD
PA1855	Phone Directory (INTRANET)
PA1856	Precinct District Voter Counts
PA1857	Preliminary Notices
PA1865	Property Tax Characteristics
PA1869	Rasscle
PA1871	Recorder Vital Records System
PA1872	Red Envelope
PA1887	SIMWIN
PA1893	Tax Rate by Tax Rate Area Search
PA1900	Tran Control Log: Shrink Wrap

PAID	NAME
PA1901	Traverse
PA1902	ARCCs AX/WX/WFM Applications
PA1905	Web Polling Place Lookup
PA1907	Kinnosa
PA1917	Chargeback System
PA1920	Sales/Deposit Permit System
PA1921	SSRS
PA1922	Training Tracking
PA1923	Countywide Customer Satisfaction Survey
PA1927	Polinsky Donor Tracking System
PA1928	EZ Access
PA1933	ARCC E-Commerce
PA1940	CMIPS Adhoc Tool
PA1971	SUN (San Diego User Network)
PA1973	ISCP - CODE 1 Plus
PA1974	ISFC - FOCUS Front-End Processing
PA1976	ISTB - Telephone Billing
PA2005	County Web Mapping Applications
PA2012	Q-Matic Line Queue Management
PA2031	Juvenile Traffic
PA2044	Public Defender Intranet (PD)
PA2056	Edgemore Nurse Staffing program
PA2057	EZ Access Interfacing Systems
PA2060	PeopleSoft HCM
PA2065	Polinsky Kids Information Data System
PA2068	Administrative Investigations Management
PA2078	TTC Mobile Home Tax Clearance Database
PA2079	Parent/Child Property Transfer System
PA2081	Property Parcel Corrections Database
PA2082	ARCC Document Management System
PA2083	Certificate Signature Printing System
PA2089	Marshall-Swift Commercial/Agricultural Estimator

PAID	NAME
PA2090	MLS
PA2093	Integrated Report Systems (I.R.S.)
PA2094	Outside Purchase Control System (OPTICS)
PA2100	EZ Access – Jwalk
PA2102	Jail Information Management System Interfaces
PA2103	JCATS Criminal Case Management System
PA2110	Vital Records Information System
PA2113	Public Health Information System
PA2115	Banknote Paper Tracking
PA2127	Prof Photocopiers
PA2134	Survey Records Imaging System
PA2135	HR Employment Document Management System
PA2144	SPS Cut
PA2150	ERP Oracle Financials
PA2152	Business Audit Tracking
PA2153	Fraud Referral Tracking System
PA2154	Secure Web Drop Box
PA2156	Bar Code File Tracking System
PA2171	NTTData Netsolutions
PA2175	SOCAT
PA2186	Elite
PA2190	SPSS
PA2191	QANET Collector System
PA2193	TTC ApplicationXtender & WebXtender
PA2200	Child Health and Disability Program/Children Youth and Families/Health Care Program for Children in Foster Care
PA2201	TTC Wausau ImageRPS
PA2202	Sharpe IPM
PA2210	Workflow Manager for Revenue and Recovery Remittance System
PA2211	ERMXtender for ARCC
PA2215	Utility Manager Pro

PAID	NAME
PA2224	Volunteer Tracking System AIS
PA2233	DIMSNET
PA2235	Probation Case Management System
PA2237	ARCC Cashiering
PA2238	Innovative Millennium
PA2239	Special Assessments by Parcel Number Search
PA2242	Buynet II
PA2245	Kronos Workforce Central
PA2250	AXAddOns
PA2257	Source Test Tracking
PA2260	Hansen for Parks & Rec
PA2261	QBIS Data Recording System (DRS)
PA2262	San Diego Immunization Registry
PA2263	OneStep Database
PA2264	Mystery Shopper
PA2265	HHSA Program Guides
PA2267	WebTrends
PA2270	External Agencies WEB Reporting
PA2273	LUEG Repository
PA2286	TTC Trustref (TTC Financial Apps)
PA2287	Viking Data Entry System
PA2288	ARCC Recording System
PA2289	ARCC Mills Act DB
PA2293	Manual Clearing Database
PA2295	Purchasing and Contracting Documentum Repository
PA2300	TTC WARP (Wire Access Request Portal)
PA2308	PHIX
PA2309	AutoCAD Raster Design
PA2313	Columbia Ultimate RPCS
PA2314	Grant or Community Enhancement
PA2315	Medical Therapy Unit Online

PAID	NAME
PA2318	ROP Mobile Home DB
PA2319	Rental Mobile Home DB
PA2324	Kofax Ascent Capture 7.0
PA2337	Case Review System
PA2340	SDE Repository
PA2341	File Tracking System
PA2343	Closed Cases Repayment Accting System
PA2344	Cal Win Interfaces
PA2351	BOS District One Website
PA2352	BOS District Two Website
PA2353	BOS District Three Website
PA2354	BOS District Four Website
PA2355	BOS District Five Website
PA2356	Applications Manager
PA2357	Accela Automation (BCMS) (LEAMS)
PA2358	COB Public Search
PA2360	PCC Staffing Database
PA2361	myRequests
PA2369	Parent Search db
PA2371	Case Folder Tracking
PA2378	WITS
PA2385	CMS Patient Eligibility System
PA2391	MaxCars
PA2397	PatternStream
PA2399	Property Profile Mapping
PA2407	Food Facility Inspection Search
PA2413	County Web Referrals
PA2415	CCS Web Referrals
PA2417	CalWIN CIS Data Mart
PA2422	Proscript
PA2427	Absentee Voter Lookup
PA2429	ArborPro Management System

PAID	NAME
PA2430	NeoGov
PA2432	Northpointe COMPAS
PA2434	Kofax Ascent Capture – FG
PA2438	TTC WITS (Web Integrated Tax System)
PA2439	APS Imaging
PA2444	Citizen Advisory Boards Application
PA2445	Cerner Millennium
PA2446	Pharmacy Outpatient System (Etreby)
PA2447	Budget Books
PA2449	QCS AdHoc Statistical Reporting Subsystem
PA2455	HR Documentum
PA2456	CWS Mandated Reporter
PA2458	Prodagio
PA2459	ERP Data Archive
PA2461	TTC CRS (Central Reporting System)
PA2462	Card Access System
PA2468	AIS Ombudsman
PA2469	AIS Case Management
PA2470	StarLIMS – Web
PA2471	BMC Footprints
PA2477	TB – Fujifilm
PA2478	TTC Bloomberg Gateway
PA2479	HHSA HR Kofax Imaging
PA2480	HHSA AIS Ombudsman Kofax Imaging
PA2481	HHSA AIS APS Kofax Imaging
PA2482	HHSA AIS Case Management Kofax Imaging
PA2483	ARCC Q-MATIC Orchestra
PA2484	ARCC Captiva Scanning Solution
PA2485	AIS-IHSS Kofax Imaging
PA2486	AIS - IHSS Documentum/Webtop
PA2489	iQCS
PA2490	Electronic Approval Workflow

PAID	NAME
PA2491	CATS Customer Dashboard
PA2492	CRM Framework
PA2493	Integrated Recording & Vital Records System (aka. ACCLAIM)
PA2494	Medical Standards In-service Tracking
PA2495	AtPac Asset Manager
PA2496	Convey 1099
PA2499	TTC iPayment Cashiering
PA2501	DCSS Data Warehouse
PA2505	Inventory and Resource Management System
PA2507	Actuate BIRT 11
PA2509	ERP Oracle Data Warehouse
PA2510	PA Enrollment
PA2511	DGS Generic Filing Cabinet
PA2512	Public Authority Payroll History
PA2514	Documentum Import Tool
PA2515	PARTS - Public Authority Registry Tracking System
PA2518	Oracle Identity Manager
PA2519	ALEX (not an acronym)
PA2520	CalWin Case Comments
PA2524	Performance Budgeting
PA2525	AuditExchange
PA2527	TTC SharePoint iTTC
PA2530	ApprMapr - Web mapping application
PA2532	Justice Electronic Library System
PA2533	Community Resource Directory
PA2534	Oracle Fusion Middleware
PA2535	TTC Ad-Hoc Bill Printing
PA2536	Care Transitions Coach System
PA2538	Public Defender eShare
PA2540	Documentum Records Manager
PA2541	Building Automation System

PAID	NAME
PA2542	ARCC SharePoint Site
PA2543	P-Card Access Database
PA2544	PCMS To HHSA Interface
PA2546	County Constituent Relationship Management
PA2548	CobbleStone Data Synchronization
PA2549	IPTS-GRM
PA2557	Crossroads Software Collision Database System
PA2558	Identity and Access Management
PA2561	Cerner CareTracker
PA2562	CalWIN ERMS
PA2563	Enterprise Document Processing Platform
PA2567	San Diego Regional Resiliency Checkup
PA2569	ROV Documentum Generic File Cabinet
PA2571	Nicus M-PWR
PA2572	Client Visit Management
PA2573	Web Application for Legacy Payroll Data and Reports
PA2574	Pyxis
PA2575	Beach and Water Quality (BWQ)
PA2576	DCSS Business Intelligence - Tableau
PA2578	County Internet Website (AEM)
PA2580	LAFCO ApplicationXtender (AX) Imaging Environment
PA2581	TTC Interactive Web Response (IWR)
PA2582	GIS Mobile Applications
PA2583	CAR
PA2584	AP Invoice Imaging System
PA2586	Enterprise Email Solution
PA2587	A&C Captiva Scanning
PA2588	PCMS Knowledge Center
PA2589	PCMS Biometrics
PA2590	DocVault

PAID	NAME
PA2592	TempTrak
PA2593	DHR Document Repository for Medical Standards
PA2594	Probation Electronic Medical Records System (PEMR)
PA2595	Granicus - Citizen Participation Suite
PA2597	SharePoint 2013 Platform
PA2598	LiveWellSD.org
PA2599	Adobe e-Forms DEH Inspections
PA2600	TTC SeeTrans
PA2601	TTC EPS Express Manager
PA2602	EPI HIE SFTP Access
PA2603	DHR Captiva7 Scanning
PA2604	Probation Contact Log Mobile Application (PUMA)
PA2605	Transform for CalWIN Checks/Warrants
PA2606	DHR Documents upload to Documentum
PA2607	Bad Check Database
PA2608	Balance Due Report DB
PA2609	eForms Repository
PA2611	CoSign Digital Signature
PA2613	TTC AEM Internet Site (SDTREASTAX.COM)
PA2614	Information Exchange Program (ConnectWellSD)
PA2615	ROV AEM Website (SDVOTE.COM)
PA2617	Probation Work Projects
PA2618	DHR BENEFITS ELECTRONIC DOCUMENTS UPLOAD
PA2619	Selectron IVR
PA2620	Facil
PA2621	Alzheimer's Project AEM Website (SDAlzheimersProject.org)
PA2622	SDPARKS AEM Website (www.sdparks.org)
PA2629	Adobe e-Forms APCD Inspections

--- End of Document ---

Appendix 4.3-2 – Audio/Video Conference Rooms Configuration and Support

Table of Contents

1. Small A/V Conference Room Configuration 3

2. Medium A/V Conference Room Configuration 4

3. Large A/V Conference Room Configuration 5

4. System Support....8

5. Construction Considerations 9

1. SMALL A/V CONFERENCE ROOM CONFIGURATION

1.1. Functionality Description

Small Conference Room that is enabled for wireless conferencing. Includes a 55" monitor display, two dongles for wireless conferencing using BYOD, HDMI at table, table box and over floor raceway, and 4K USB Camera with microphone.

1.2. Display

- A 55" display monitor will fit room dimension of approximately 16x12 up to 18x14
- Display mounted on wall with an articulating arm to allow easy servicing of equipment mounted behind display
- Small device mounting system

1.3. Source Devices

- 1 Camera mounted above the display
- 1 Dongle base unit mounted behind display
- 2 Dongles for BYOD connectivity to the display and camera
- 1 Receiver mounted behind display
- 1 Transmitter mounted under table
- 1 Table box for HDMI cable to pass through

1.4. Audio

- 1 Array microphone built into the camera to allow far end to hear
- 1 Set of display speakers will allow program audio and far end audio to be heard in the room

1.5. System Components

Components subject to change and be replaced with equal or better products:

Component Description	Qty
55IN COMMERCIAL 4K UHD LED LCD MNTR DISPLAY 350 NIT VNWeight: 53.00 Dim	1
THIN SWING ARM (LARGE)	1
PROXMOUNT PLATE9X12	1
CLICKSHARE Wireless Presentation System	1
DM Lite – HD Scaling Auto-Switcher & HDMI® over CATx Extender 400	1
IQ Camera	1
DIGITALINX SECURE ADAPTER RING	1
HDMI PREMIUM 18G CBL W/NET 3'	2
3FT CAT6 SNAGLESS UTP CAB	1

Component Description	Qty
FlipTop™ FT2 Series, 202 Size, Mechanical, Black, 6 Module Slots	1
AC Power Outlet Module for FT2 Series, Triple, US NEMA 5, Type B, w/2 Under-Table Outlets & Cord	1
USB Rapid Charging Module for FT2 ELEC Series, USB Type-C & Type-A High Power Charging Ports, Bus Po	1
Pass-Through Cable for FT2 Series, HDMI® to HDMI, 18 Gbps, 8 ft (2.4 m)	1
Wireless conference speaker (DECT), base unit, battery pack, power supply charger and connecting cable	1
OFR BASE AND COVER	1
OVER FLOOR RCWY 2GANG BOX	1
OFR DUPLEX PLATE	1
OFR DECORATOR PLATE	1
OFR IN-WALL END FITTING	1
DECOR INSERT PLATE 2PORT WHT	1
INSERT BLANK WHT	1
RJ45 INSERT CAT6A SH 180	1

2. MEDIUM A/V CONFERENCE ROOM CONFIGURATION

2.1. Functionality Description

Medium Conference Room that is enabled for wireless conferencing. Includes one 85" display monitor, two dongles for wireless conferencing using BYOD, HDMI at table, two table boxes and over floor raceway, and 4K USB Camera with microphone.

2.2. Display

- One 85" Displays will fit room dimensions of approximately 24x13 up to 26x14
- Display will be mounted on wall
- Pull-Out small device mounting system

2.3. Source Devices

- 1 Camera mounted above the display
- BYOD PC mounted behind display
- 1 Dongle base unit mounted behind display
- 2 Dongles for BYOD connectivity to the display and camera
- 1 Wireless keyboard and mouse provided for computer
- 1 Receiver mounted behind display
- 1 Transmitter mounted under table
- 1 HDMI distribution amplifier provided to drive both displays

- 1 Table box for HDMI cable to pass through
- 1 Table box for power and USB charging

2.4. Audio

- 1 Array microphone built into the camera will allow the far end to hear the room participants
- 1 Display speakers will allow program audio and far end audio to be heard throughout the room

2.5. System Components

Components subject to change and be replaced with equal or better products:

Description	Qty
85IN COMMERCIAL 4K UHD LED WIFIMNTR	1
Micro-Adjust Fixed Wall Mount X-Large	1
PROXSLIDE PLT15X10	1
CLICKSHARE Wireless Presentation System	1
DM Lite – HD Scaling Auto-Switcher & HDMI® over CATx Extender 400	1
IQ Camera	1
DIGITALINX SECURE ADAPTER RING	1
HDMI PREMIUM 18G CBL W/NET 3'	2
3FT CAT6 SNAGLESS UTP CAB	1
FlipTop™ FT2 Series, 202 Size, Mechanical, Black, 6 Module Slots	2
AC Power Outlet Module for FT2 Series, Triple, US NEMA 5, Type B, w/2 Under-Table Outlets & Cord	2
USB Rapid Charging Module for FT2 ELEC Series, USB Type-C & Type-A High Power Charging Ports, Bus Po	4
Pass-Through Cable for FT2 Series, HDMI® to HDMI, 18 Gbps, 8 ft (2.4 m)	1
Wireless conference speaker (DECT), base unit, battery pack, power supply charger and connecting cable	1
OFR BASE AND COVER	1
OVER FLOOR RCWY 2GANG BOX	1
OFR DUPLEX PLATE	1
OFR DECORATOR PLATE	1
OFR IN-WALL END FITTING	1
DECOR INSERT PLATE 2PORT WHT	1
INSERT BLANK WHT	1
RJ45 INSERT CAT6A SH 180	1

3. LARGE A/V CONFERENCE ROOM CONFIGURATION

3.1. Functionality Description

Large Simple Conference Room that is enabled for wireless conferencing. Includes a 6000 lumen projector and fixed frame 130” screen, two dongles for wireless conferencing using BYOD, HDMI at table, three

table boxes and over floor raceway, 4K USB Camera with microphone, and a ceiling beam tracking microphones and ceiling speakers.

3.2. Display

- A 6000-lumen laser projector and 130" fixed frame screen will fit room dimensions of approximately 32x13 up to 34x14
- Projector will be ceiling mounted with above ceiling equipment storage
- Projection screen mounted on wall

3.3. Source Devices

- 1 Camera mounted below the screen
- 1 In-wall recessed camera box to house the camera and the USB 3.0 extender
- 1 Dongle base unit mounted on top of projector
- 2 Dongles for BYOD connectivity to the projector and camera
- 1 Receiver mounted in above ceiling equipment box at projector location
- 1 Transmitter mounted under table
- 1 Table box will be provided for HDMI cable to pass through
- 2 Table boxes provided for power and USB charging

3.4. Audio

- Beam tracking ceiling microphones will allow far end to hear room participants
- Ceiling speakers will allow program audio and far end audio to be heard in throughout room
- An audio DSP will be installed and programmed

3.5. System Components

Components subject to change and be replaced with equal or better products:

Description	Qty
Pro L1060U Laser Projector, 6000 Lumens, WUXGA, White	1
UTB CONTOURAE BLACK HDC1.1 130D	1
UNIVERSAL RPMA	1
CEILING STORAGE BOX 2X2 W/COLUMN W/POWER	1
ADJ. PIPE 24" TO 36"	1
CLICKSHARE Wireless Presentation System	1
DM Lite – HD Scaling Auto-Switcher & HDMI® over CATx Extender 400	1
IQ Camera	1
USB 3-2-1 RAVEN 3104 - NA, 4 P	1
IN-WALL ENCLOSURE FOR VC CAMERAS	1
DIGITALINX SECURE ADAPTER RING	1

Description	Qty
HDMI PREMIUM 18G CBL W/NET 3'	2
3FT CAT6 SNAGLESS UTP CAB	1
Fixed I/O DSP with 12 analog inputs, 8 analog outputs, 8 channels configurable USB audio, 128 x 128	1
Gigabit PoE+ Injector, IEEE802.3af compliant, IEEE802.3at classified, 90-264 VAC Input Volta	1
AVB Beamtracking ceiling microphone with PoE+ amplifier, white surface mount	1
Expansion AVB Beamtracking ceiling microphone, white surface mount	1
Saros® Integrator 6.5” 2-Way In-Ceiling Speaker, White Textured, Single (must be ordered in multiple	4
FlipTop™ FT2 Series, 202 Size, Mechanical, Black, 6 Module Slots	3
AC Power Outlet Module for FT2 Series, Triple, US NEMA 5, Type B, w/2 Under-Table Outlets & Cord	3
USB Rapid Charging Module for FT2 ELEC Series, USB Type-C & Type-A High Power Charging Ports, Bus Po	6
Pass-Through Cable for FT2 Series, HDMI® to HDMI, 18 Gbps, 8 ft (2.4 m)	1
OFR BASE AND COVER	1
OVER FLOOR RCWY 2GANG BOX	1
OFR DUPLEX PLATE	1
OFR DECORATOR PLATE	1
OFR IN-WALL END FITTING	1
DECOR INSERT PLATE 2PORT WHT	1
INSERT BLANK WHT	1
RJ45 INSERT CAT6A SH 180	1

4. SYSTEM SUPPORT

4.1. System Support on the System shall be provided for 3 years from the date of installation in accordance with the terms set forth below.Definitions

4.1.1. System – the components which make up the Small, Medium and Large Simple Conference Rooms as listed in this Schedule, with the exception of Consumables and Obsolete Equipment outside the initial 3-Year support period.

4.1.2. Business Hours – Monday to Friday, 8:00AM – 5:00PM PST, excluding County holidays.

4.1.3. Obsolete Equipment – system components (though possibly still in use) that are no longer made and/or supported by manufacturer, or products with formal end of life as defined by their manufacturer.

4.1.4. Consumables – parts such as recording media, batteries, projection lamps and diskettes.

4.2. System Recertification

Two on-site scheduled recertification sessions per year (from install date) to perform necessary cleaning, adjustments, functional tests, replacement of parts, and repairs to keep the equipment in good and efficient operating condition.

4.3. Training

On-site training, provided on an as needed basis but no more than once per quarter, to ensure that system users understand the system functionality and how to operate it. The training must be scheduled at least 2 weeks in advance.

4.4. Asset Tracking

Management of the system's individual electronic components and reporting of description, model, serial numbers, in-service dates, and physical location.

4.5. Technical Support

4.5.1. Priority Support by Phone – response within 2 business hours during Business Hours.

4.5.2. Priority Support Onsite – response within 8 business hours to perform troubleshooting, to localize and diagnose faults where the onsite location is within 60-mile radius of support center location, while 24 business hours if outside the 60 mile radius.

4.5.3. Repair or replacement of faulty equipment with exclusion of Obsolete Equipment that is outside the initial 3-Year support period.

4.5.4. Provision of materials and repair parts excluding Consumables.

4.5.5. Software updates.

4.5.6. Loaner Equipment when repair or replacement cannot be completed or provided within a Business Day. This is limited to tabletop LCD projectors and flat screen monitors under 50". Tabletop projectors are not integrated into a system. Flat screen monitors will be installed onto a wall if reasonably possible.

4.5.7. Recycling of system equipment and Consumables.

5. CONSTRUCTION CONSIDERATIONS

5.1. The County will be responsible for coordinating and paying for the necessary modifications to the room as directed by Contractor. The costs associated with any modifications are not included in Contractor's scope of work. The following work is not included in the Small, Medium and Large Simple Conference Rooms Resource Units:

- All conduits, high voltage, wiring panels, breakers, relays, boxes, receptacles, etc.
- Concrete saw cutting and/or core drilling
- Fire wall, ceiling, roof and floor penetration
- Necessary gypsum board replacement and/or repair
- Necessary ceiling tile or T-bar modifications, replacements and/or repair
- Structural support of equipment
- Installation of ceiling mounted projection screen
- All millwork (moldings, trim, cut outs, etc.)

- Patching and Painting
- Permits

5.2. The following are Contractor's Assumptions:

- Contractor shall assign a Project Coordinator to manage installation of Small, Medium and Large Conference Room from start to finish.
- Room(s) match(es) the drawings provided by County.
- Site preparation by the County includes electrical and data placement per System specification.
- Site preparation will be verified by Contractor project coordinator prior to installation being scheduled.
- All work areas should be clean and dust free prior to the beginning of on-site installation of electronic equipment.
- County communication of readiness will be considered accurate and executable by Contractor project coordinator.
- There is ready access to the building / facility and the room(s) for equipment and materials.
- There is secure storage available for equipment during a multi-day installation.
- County provided equipment (e.g., laptop) and existing cabling are in good working condition and will integrate into the designed solution. Any necessary repair, replacement and/or configuration of these items will be made at an additional cost to County.
- All network configurations including IP addresses are to be provided, operational and functional before installation begins.
- Cable or satellite drops must be in place with converter boxes operational before the completion of installation.
- Document review, feedback on drawings and response to correspondence will be provided by the County within seven business days or as agreed upon with Contractor.

END OF SCHEDULE

Schedule 4.4 – Asset Management Upgrades and Enhancements

Table of Contents

1. Overview 3

2. Methodology 3

1. OVERVIEW

Contractor shall provide the technology management and upgrade/refresh services necessary to maintain all Hardware and Software used by the County in connection with the Services at manufacturers' current levels and releases to meet the County's ongoing functional and performance requirements and to maintain a current, stable, and productive working environment.

2. METHODOLOGY

2.1. Contractor shall conduct Hardware refreshes on all Hardware Assets provided by the Contractor (including Purchased Assets) based on cycles described in the appropriate Service Framework sections of Schedule 4.3. Unless otherwise indicated in Schedule 4.3, a "hardware refresh" means a complete, full box replacement (i.e. a new serial number). Certain exceptions apply, as more fully described in Schedule 4.3.

2.2. Contractor shall maintain currency on all Software Assets provided by Contractor, including any Purchased Assets that are Software, and shall upgrade such Software Assets to the latest commercially available version of the Software no later than one (1) year after the release date, unless otherwise approved by the County.

2.3. Notwithstanding anything in part 2.2 above to the contrary, Contractor shall promptly provide all security patches, service packs and other maintenance releases for Software provided by Contractor (including any Purchased Assets that are Software) as soon as such patches, packs or releases are made commercially available.

2.4. Contractor shall provide a deployment plan and communication plan to include impacted applications and business departments.

END OF SCHEDULE

Schedule 4.8 – Service Levels

Table of Contents

1 Overview 5
2 High Level Requirements 5
3 Incident Service Level Severities 5
3.1 Incident Service Level Reporting Exclusions 6
4 Output Delivery Schedules 7
5 Service Level Summarization and Weighting Factors 8
6 Cross Functional Service Levels 14
6.1 Severity 1 Incidents 14
6.2 Severity 2 Incidents 15
6.3 Severity 3 Incidents 16
6.4 Severity 4 Incidents 17
6.5 Add/Modify End-User Account 18
6.6 Add/Modify End-User Account (Interim) 20
6.7 Terminate End-User Account 23
6.8 Budgetary Estimate Request 25
6.9 Project Estimate Request 26
6.10 Accuracy of Chargeback Billing 27
6.11 Annual Disaster Recovery (DR) Test 28
6.12 Application Recovery Post-Disaster 29
6.13 Asset Tracking 30
6.14 Root Cause Analysis 32
6.15 Key Personnel Vacant Position 33
7 Service Desk Service Levels 34
7.1 Incident Resolution Confirmation Notice 34
7.2 Password Reset Completion 35
7.3 Response Time 36

7.4 Service Repair Scheduling....38
7.5 Customer Satisfaction....39
7.6 First Call Resolution....40
7.7 First Call Resolution – 2nd Generation....41
8 End-User Service Levels....42
8.1 Critical Software Patches....42
8.2 Software IMAR....46
8.3 Hardware IMAR....48
8.4 OIC Additions, Updates and Removals....50
9 Network Service Levels....51
9.1 Transaction Response Time — Internet/Intranet Access....51
9.2 Transaction Response Time – Data Center....52
9.3 Voice System Call Blocking....53
9.4 Data Network Availability....54
9.5 Internet Availability....56
9.6 Voice Network Availability....57
10 Data Center Service Levels....58
10.1 Output Delivery....58
10.2 Daily Backup....59
10.3 Quarterly Backup / Restore....60
10.4 Data Restore....61
10.5 Server Decommission....62
10.6 Server Provisioning....63
10.7 [Reserved]....64
10.8 [Reserved]....65
10.9 [Reserved]....66
10.10 [Reserved]....67

10.11 Server Software Update....68
10.12 Server Availability....75
11 Applications Service Levels....77
11.1 Project Management Plan Rework....77
11.2 Service Request Schedule Performance....79
11.3 Variance to Application Budget....80
11.4 Application Availability....81
11.5 Application Availability (Priority 1)....82
11.6 Application Availability (Priority 2)....83
11.7 Application Availability (Priority 3)....84
11.8 Documentation Update Accuracy....85
11.9 Application Response Time....89
11.10 Root Cause Analysis Action Closure....91
12 Transition Service Levels....92
13 Special Requirements....92
14 Network Credit Table Examples....92

1 OVERVIEW

Each Service Level has been created to identify key performance measures that will be used to evaluate Contractor's delivery of Services. The overriding goal in developing Service Levels is to monitor and measure performance of the County's most significant business requirements. The expectation is that new Service Levels will be added, deleted or changed to reflect changing or new business requirements. The continuous improvement in effective and reliable provision of Services for Service Levels on yearly basis is expected.

2 HIGH LEVEL REQUIREMENTS

2.1. Contractor shall post all Service Levels reports to the Service Portal.

2.2. Contractor shall maintain a live and up-to-date dashboard of current, selected Service Levels on the Service Portal.

2.3. Contractor shall immediately respond to requests for Services from the offices of the Chief Administrative Office (CAO) and Board of Supervisors (BOS) by dispatching personnel onsite. Site visits will be coordinated through the County Technology Office representative.

3 INCIDENT SERVICE LEVEL SEVERITIES

Severity	Description	Definition
1	Critical	Incidents that cause a complete and immediate work stoppage affecting a Priority 1 Application affecting multiple users. Any single-user Incident involving a Priority 1 Application will be handled operationally as a Severity 1 but will be reported as a Severity 4. In addition, any Incident related to life, health or safety Sites, including but not limited to, the following: • Polinsky Center (entire site data system) or Auto Attendant • Rosecrans Psych Hospital (entire site Data System) • Edgemoor Hospital (entire site data system)

Severity	Description	Definition
2	Urgent	Incidents that cause a complete and immediate work stoppage affecting a Priority 2 Application affecting multiple users. In addition, any Service Request meeting the following criteria: • All Data or Voice down at any County Site • Auto Attendants or ACDs • Video teleconferencing systems located at the Probation Department and Public Defender • Internet access (entire County) • Intranet access (entire County) • File Services (more than one (1) user) • Print Services (more than one (1) user) • E-mail Services (more than one (1) user) • Security violation • Identity management system (more than one (1) user) • Any Interactive Voice System (IVS) Application • Toll-free number • Remote access Service (more than one (1) user) • County badge reader system (entire system only)
3	Important	Incidents that cause a complete and immediate work stoppage affecting a Priority 3 Application affecting multiple users. In addition, any Service Request meeting the following criteria: • Jail Blue Phones • Voice mail system (more than one (1) user) • Audio systems • All other video teleconferencing systems • Alarm circuits • SCADA monitoring circuits • Any non-priority 1 or 2 multiple-user Incident
4	Low	An Incident that affects a single End-User's ability to perform his/her normal daily activities.

3.1 Incident Service Level Reporting Exclusions

Tickets pertaining to the following shall not be included in the calculations for the Incident Service Levels:

- Status Tickets
- Internal Contractor Tickets
    - The exclusion of internal contractor tickets will not result in the exclusion of any End-User generated tickets with the same root cause.
- Duplicate tickets directly related to a master ticket

- Power Outage time will be excluded unless the Contractor is responsible for directly or indirectly causing the power outage.
- Equipment and circuits funded through the E-Rate Program used for internet access by public visitors at the County to the San Diego County Branch Libraries.

4 OUTPUT DELIVERY SCHEDULES

The distribution of reports by Contractor for managed print Services (as set forth in the Data Center Services Framework) shall be in accordance with the following schedule:

Location Description	Trips / Day	Drop Points / Location	Delivery Days	Delivery Time(s) No Later Than
County Administration Center 1600 Pacific Coast Highway Mail Room 050	1	1	Monday – Friday	9:00 AM
County Operations Center 5560 Overland Dr Suite 180 & 5530 Overland Dr Suite 410	1	2	Monday - Friday	9:00 AM
San Diego County Jail 1173 Front St	1	1	Monday - Friday	9:00 AM
Downtown Courthouse Hall of Justice 220 West Broadway	1	1	Monday - Friday	7:30 AM
San Diego Superior Court-Kearny Mesa 8950 Clairemont Mesa Boulevard	1	1	Monday - Friday	7:30 AM
Vista Superior Court 325 South Melrose Dr	1	1	Monday - Friday	7:30 AM

5 SERVICE LEVEL SUMMARIZATION AND WEIGHTING FACTORS

The Service Levels are summarized in the table below. Service Level weighting factors apply as indicated in the table below. The County will adjust Weighting Factors in accordance with Schedule 16.8.

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
	Cross Functional	Severity 1 (S1) Incidents	
1		1A – S1 Incidents Revolved in ≤ 4 hours	13%
2		1B – S1 Incidents Revolved in ≤ 8 hours	9%
3		1C – Average of 4% of total S1 Incidents with longest resolution times	3%
	Cross Functional	Severity 2 (S2) Incidents	
4		2A – S2 Incidents Revolved in ≤ 6 hours	12%
5		2B– S2 Incidents Revolved in ≤ 10 hours	8%
6		2C – Average of 4% of total S2 Incidents with longest resolution times	3%
	Cross Functional	Severity 3 (S3) Incidents	
7		3A – S3 Incidents Revolved in ≤ 8 hours	7%
8		3B – S3 Incidents Revolved in ≤ 12 hours	3%
9		3C – Average of 4% of total S3 Incidents with longest resolution times	1%
	Cross Functional	Severity 4 (S4) Incidents	
10		4A – S4 Incidents Revolved in ≤ 10 hours	11%
11		4B – S4 Incidents Revolved in ≤ 16 hours	5%
12		4C – Average of 4% of total S3 Incidents with longest resolution times	2%
13	Cross Functional	Add End-User Account	0%

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
13-1	Cross Functional	Add End-User Account (Interim)	
		13-1a – 3 Business Days	3%
		13-1b – 5 Business Days	
		13-1c - Edgemoor NetSolutions application	n/a
14	Cross Functional	Terminate End-User	3%
15	Cross Functional	Budgetary Estimate Request	3%
16	Cross Functional	Project Estimate Request	3%
17	Cross Functional	Accuracy of Chargeback Billing	4%
18	Cross Functional	Annual Disaster Recovery (DR) Test	0%
19	Cross Functional	Application Recovery Post-Disaster	0%
20	Cross Functional	Asset Tracking	0%
21	Cross Functional	Root Cause Analysis	3%
22	Cross Functional	Filling Vacant Key Personnel Positions	3%
55	Cross Functional	Root Cause Analysis Corrective and Preventative Action Completion	6%
23	Service Desk	Incident Resolution Confirmation Notice	3%
24	Service Desk	Password Resets	
		24a – Password Resets within 30 minutes	3%
		24b – Password Resets within 60 minutes	
25	Service Desk	Response Time	
		A – Speed-to-Answer Time in 75 seconds	3%
		B – Speed-to-Answer Time in 90 seconds	

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
		C – Call Abandonment Rate	
		D – Email Response Time	
		E – Voice Mail Response Time	
26	Service Desk	Service Repair Scheduling	3%
27	Service Desk	Customer Satisfaction	4%
28	Service Desk	First Call Resolution	0%
54	Service Desk	First Call Resolution – 2nd Generation	3%
29-1	End-User	Operating System (OS)/Microsoft Office Patches Involving Technical Issues and Security Vulnerabilities	3%
29-2	End-User	Operating System (OS) and Core Software Patching for Critical and Zero Day Vulnerabilities	
29-3	End-User	Core Software Patching Involving Technical Issues and Security Vulnerabilities	
30	End-User	Software IMAR	4%
		30a – Software License Available	
		30b – Software License Not Available	
		30c – Move/Remove	
31	End-User	Hardware IMAR	3%
		31a – Hardware License Available	
		31b – Hardware License Not Available	
		31c – Move/Remove	
32	End-User	OIC Additions and Removals	3%
33	Network	Transaction Response Time – Internet/Intranet Availability	

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
		33a – Transaction Response Time – Intranet within 0.5 seconds	3%
		33b – Transaction Response Time – Intranet within 0.75 seconds	
34	Network	Transaction Response Time – Data Center	
		34a – Transaction Response Time – Data Center within 1 second	3%
		34b – Transaction Response Time – Data Center within 3 seconds	
35	Network	Voice System Call Blocking	3%
36	Network	Data Network Availability	
		36a – Average Availability	3%
		36b – Individual Site via Fiber	
		36c – Individual Site via Copper	
37	Network	Internet Availability	3%
38	Network	Voice Network Availability	3%
39	Data Center	Output Delivery	3%
40	Data Center	Daily Backup	3%
41	Data Center	Quarterly Backup/Restore Test	0%
42	Data Center	Data Restore	
		42a – Data 30 days old or less	1%
		42b – Data 31 days old or more	
43	Data Center	Server Decommission	3%
44	Data Center	[Reserved]	0%
44-1	Data Center	Server Provisioning – Physical (Excludes Oracle)	0%

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
44-2	Data Center	Server Provisioning – Virtual	2%
44-3	Data Center	Server Provisioning – Oracle	2%
45	Data Center	[Reserved]	
46	Data Center	Server Software Update	
		46-1 – Server Software Update - Operating system patching and updates for Windows and Linux servers	2%
		46-2 – Server Software Update - Operating system patching for Solaris and AIX servers	
		46-3 – Server Software Update - Operating System Patching for Critical and Zero Day Vulnerabilities	1%
		46-4 – Server Software Update - Middleware patching for Production PAIDs	1.5%
		46-5 – Server Software Update - Application Patching for Production PAIDs	1.5%
47	Data Center	Server Availability	3%
48	Applications	Project Management Plan Rework	2%
49	Applications	Service Request Schedule Performance	6%
50	Applications	Variance to Application Budget	6%
51	Applications	Application Availability	
	Applications	51-1 – Application Availability (P1)	1.7%
	Applications	51-2 – Application Availability (P2)	1.7%
	Applications	51-3 – Application Availability (P3)	1.6%
52	Applications	Documentation Update Accuracy	3%

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
53	Applications	Application Response Time	0%
		53a – Application Response Time – Priority 1 Applications	
		53b – Application Response Time – Priority 2 Applications	
		53c – Application Response Time – Priority 3 Applications	

6 CROSS FUNCTIONAL SERVICE LEVELS

6.1 Severity 1 Incidents

Service Level	Severity 1 Incidents		
Service Level ID	1, 2, 3		
Definition	Time to restore service from time of Incident report to Service Desk Note: Any S1 incident whose duration > 4 or 8 hours, and time exclusions were taken by Contractor, are subject to review/approval by the County. Any exceptions taken shall be reported with the monthly SL reports and maintained by Contractor.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent of incidents resolved for D1, D2 and D3 designation	**1A:** D1 = S1 incidents resolved ≤ 4 hours **1B:** D2 = S1 incidents resolved ≤ 8 hours **1C:** D3 = average of 4% of the total S1 incidents with longest resolution times	D1 ≥ 91% of total S1 incidents for Month D2 ≥ 96% of total S1 incidents for Month D3 ≤ 16 hours	D1 ≥ 95.5% D2 ≥ 98% Same formula but modified to 2% of the total S1 incidents with longest resolution times
Formula	**1A:** (Total S1 incidents per Month resolved ≤ 4 hours / total S1 incidents) **1B:** (Total S1 incidents per Month resolved ≤ 8 hours / total S1 incidents) **1C:** Average of 4% of S1 Incidents per Month with longest restore time		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Ticket Duration: Service Desk receipt through service restoration		

6.2 Severity 2 Incidents

Service Level	Severity 2 Incidents		
Service Level ID	4, 5, 6		
Definition	Time to restore service from time of Incident report to Service Desk Note: Any S2 incident whose duration > 6 or 10 hours, and time exclusions were taken by Contractor, are subject to review/approval by the County. Any exceptions taken shall be reported with the monthly SL reports and maintained by Contractor.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent of incidents resolved for D1, D2 and D3 designation	**2A:** D1 = S2 incidents resolved ≤ 6 hours **2B:** D2 = S2 incidents resolved ≤ 10 hours **2C:** D3 = average of 4% of the total S2 incidents with longest resolution times	D1 ≥ 91% of total S2 incidents for Month D2 ≥ 96% of total S2 incidents for Month D3 ≤ 20 hours	D1 ≥ 95.5% D2 ≥ 98% Same formula but modified to 2% of the total S2 incidents with longest resolution times
Formula	**2A:** (Total S2 incidents per Month resolved ≤ 6 hours / total S2 incidents) **2B:** (Total S2 incidents per Month resolved ≤ 10 hours / total S2 incidents) **2C:** Average of 4% of S2 Incidents per Month with longest restore time		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Ticket Duration: Service Desk receipt through service restoration		

6.3 Severity 3 Incidents

Service Level	Severity 3 Incidents		
Service Level ID	7, 8, 9		
Definition	Time to restore service from time of Incident report to Service Desk		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent of incidents resolved for D1, D2 and D3 designation	**3A:** D1 = S3 incidents resolved ≤ 8 hours **3B:** D2 = S3 incidents resolved ≤ 12 hours **3C:** D3 = average of 4% of the total S3 incidents with longest resolution times	D1 ≥ 92% of total S3 incidents for Month D2 ≥ 96% of total S3 incidents for Month D3 ≤ 24 hours	D1 ≥ 96% D2 ≥ 98% Same formula but modified to 2% of the total S3 incidents with longest resolution times
Formula	**3A:** (Total S3 incidents per Month resolved ≤ 8 hours / Total S3 incidents) **3B:** (Total S3 incidents per Month resolved ≤ 12 hours / Total S3 incidents) **3C:** Average of 4% of S3 Incidents per Month with longest restore time		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Ticket Duration: Service Desk receipt through service restoration		

6.4 Severity 4 Incidents

Service Level	Severity 4 Incidents		
Service Level ID	10, 11, 12		
Definition	Time to restore service from time of Incident report to Service Desk		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent of incidents resolved for D1, D2 and D3 designation	**4A:** D1 = S4 incidents resolved ≤ 10 hours **4B:** D2 = S4 incidents resolved ≤ 16 hours **4C:** D3 = average of 4% of the total S4 incidents with longest resolution times 6 AM to 6 PM Monday-Friday, excluding the County's holidays	D1 ≥ 92% of Total S4 incidents for Month D2 ≥ 96% of Total S4 incidents for Month D3 ≤ 32 hours	D1 ≥ 96% D2 ≥ 98% Same formula but modified to 2% of the total S4 incidents with longest resolution times
Formula	**4A:** (Total S4 incidents per Month resolved ≤ 10 hours / total S4 incidents) **4B:** (Total S4 incidents per Month resolved ≤ 16 hours / total S4 incidents) **4C:** Average of 4% of S4 Incidents per Month with longest restore time		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Ticket Duration: Service Desk receipt through service restoration		

6.5 Add/Modify End-User Account

Service Level	Time duration for creation of and/or changes to End-User account from time of Service Request		
Service Level ID	13		
Definition	Measures the time to add and/or modify new End-User account		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
End-User account addition or modification Service Request completed	3 business days or by the date described in the Service Request or scheduled due date	90%	95%
Formula	Number of End-User Account creation requests completed within Performance Target/total number End-User Account creations requested Algorithm: 100 x ((A – E) / (B – D)) >= 90% where A – # of requests for account and/or access creation and/or change completed within 3 business days or by date described in the service request or by scheduled due date (# Traditional + # Automated CSRF + # Peoplesoft) B – Total # of requests for account and/or access creation and/or change (# Traditional + # Automated CSRF + # Peoplesoft) D – # of requests for account and/or access creation and/or change for non-County employees (i.e. external agencies, Contractor staff, Contractor managed vendors) (# Traditional + # Automated CSRF) E – For non-County employees (i.e. external agencies, Contractor staff, Contractor managed vendors) (# Traditional + # Automated CSRF), # of requests for account and/or access creation and/or change completed within 3 business days or by date described in the service request or by scheduled due date. Clock starts when: • Parent ticket and line items created by Help Desk or Automated CSRF Workflow for account creation and/or		

	access requests to be processed via manual provisioning and any incomplete items or items open to interpretation resolved • Request approved and released by Automated CSRF Workflow for account creation and/or access requests to be processed via automated provisioning • Request released by Peoplesoft for account creation and default access defined per the PeopleSoft business rules to be processed via automated provisioning
	Requests for User IDs received from the same County department on the same day, in excess of twenty (20) or more, an Contractor team member will contact the requestor to determine the required delivery date for some or all of the User IDs requested, and/or solicit approval for an exception from the CIO or designee.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Contractor-provided

6.6 Add/Modify End-User Account (Interim)

Service Level	Time duration for creation of and/or changes to End-User account from time of Service Request (SR)		
Service Level ID	13-1		
Definition	Measures the time to add and/or modify new End-User account		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
End-User account addition or modification SR completion	13-1a. 3 business days or by the date described in the SR or scheduled due date	13-1a. 60%	13-1a. 80%
	13-1b. 5 business days or by the date described in the SR or scheduled due date	13-1b. 95%	13-1b. 97.5%
	13-1c. Edgemoor NetSolutions application - 1 hour from the receipt of the SR from the receipt of the SR during business hours (8:00am - 5:00pm Mon-Fri)	N/A	N/A

Formula	13-1a. Total # of requests for account and/or access creation and/or change completed within 3 business days or by date described in the service request or by scheduled due date divided by number of requests >= 60% **Algorithm:** 100 x ((A – E) / (B – D)) >= 60% where A – # of requests for account and/or access creation and/or change completed within 3 business days or by date described in the service request or by scheduled due date B – Total # of requests for account and/or access creation and/or change D – # of requests for account and/or access creation and/or change for non-County employees (i.e. external agencies, Contractor staff, Contractor managed vendors) E – For non-County employees (i.e. external agencies, Contractor staff, Contractor managed vendors), # of requests for account and/or access creation and/or change completed within 3 business days or by date described in the service request or by scheduled due date. 13-1b. Total # of requests for account and/or access creation and/or change completed within 5 business days or by date described in the service request or by scheduled due date divided by number of requests >= 95% **Algorithm:** 100 x ((A – E) / (B – D)) >= 95% where

	A – # of requests for account and/or access creation and/or change completed within 5 business days or by date described in the service request or by scheduled due date B – Total # of requests for account and/or access creation and/or change D – # of requests for account and/or access creation and/or change for non-County employees (i.e. external agencies, Contractor staff, Contractor managed vendors) E – For non-County employees (i.e. external agencies, Contractor staff, Contractor managed vendors), # of requests for account and/or access creation and/or change completed within 5 business days or by date described in the service request or by scheduled due date. For clarity, only 13-1a and 13-1b must be met for this Service Level. 13-1c will not be measured for SL purposes. Clock starts when parent ticket and line items created by Service for account creation and/or access requests to be processed via manual provisioning and any incomplete items or items open to interpretation resolved. Requests for User IDs received from the same County department on the same day, in excess of twenty (20) or more, Contractor team member will contact the requestor to determine the required delivery date for some or all of the User IDs requested, and/or solicit approval for an exception from the CIO or designee.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Contractor-provided

6.7 Terminate End-User Account

Service Level	Time duration for termination of End-User account from time of authorized request by County.		
Service Level ID	14		
Definition	Time duration from the County authorized request to the termination of End-User authorized access for the organization or Contractor.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
End-User deletion Service Request completed	1 business day or by requested due date*	98%	99%
Formula	End-User account termination requests completed within Performance Target / Total End-User account deletion requests. **Algorithm:** 100 x ((A – C – D – E – F) / (B – C – D – E – F)) >= 98% where **Inclusions:** A – # of requests for account termination completed within 1 business day or by requested due date B – Total # of requests for account terminations **Exclusions:** C – # of requests without request for account termination, i.e., those requests with only access removal D – # of requests for non-County employees (i.e., external agencies, Contractor staff, Contractor managed vendors) E – # of requests for bulk user terminations (over 20 users on one request) F – * # of requests for which the requested due date is prior to request approval, or less than 1 business day Clock starts when ticketing system termination tasks are created by the Service Desk or as a part of a Ticketing system workflow.		

	a) For End-User account terminations, County business rules dictate the Active Directory account be disabled and retained for 2 years prior to deletion. For SL purposes, the disabling of the Active Directory account is counted. b) Request for access deletions that are not a termination are not included
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	The ticketing tool supplied by Contractor automatically records date and time stamps for each activity within a process.

6.8 Budgetary Estimate Request

Service Level	Time Duration to complete a Budgetary Estimate		
Service Level ID	15		
Definition	Length of time to provide budget estimate in response to Service Requests, including schedule and cost estimates or make contact with Requester to negotiate a Budgetary Estimate delivery date for Service Requests.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Request Completion	Proposal for Development completed within 5 business days	95%	97.5%
Formula	**Proposal for Development = 100 x (C/D)** (C) = Total Proposal for Development Completed within 5 business days (D) = Total Proposal for Development requested		
Measurement Interval	Daily		
Reporting Period	Monthly		
Measurement Tool/Source Data	Proposal for Development completed within 5 business days or as negotiated with requestor		

6.9 Project Estimate Request

Service Level	Time Duration to complete a Project Estimate		
Service Level ID	16		
Definition	Length of time to provide a Project Estimate in response to a Project Estimate Service Request, including schedule and costs estimates or make contact with Requester to negotiate a Project Estimate delivery date for Service Requests. Time excludes any County incurred time needed to update/define requirements needed to complete the estimate.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Request Completion	10 business days or as negotiated	95%	97.5%
Formula	Number of Project Estimate requests submitted within target/Total number of Project Estimate requests		
Measurement Interval	Daily		
Reporting Period	Monthly		
Measurement Tool/Source Data	Project Estimates completed within 10 business days or as negotiated with requestor		

6.10 Accuracy of Chargeback Billing

Service Level	Accuracy of billing: chargeback billing accuracy		
Service Level ID	17		
Definition	Measures the accuracy of chargeback billing		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Accuracy	Valid charges and credits	98%	99%
Formula	(Total number of charges – Number of disputed charges resolved in County favor – Low Org change requests not executed) / Total number of charges A rate error impacting more than one chargeback item is counted as a single error. Low Org requests not executed are counted as individual errors.		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	ITrack Chargeback Data and Change Requests • Disputed Charges are those submitted via ITrack as Delete requests. • Low Org Change Requests are those submitted via ITrack Move requests.		

6.11 Annual Disaster Recovery (DR) Test

Service Level	Annual test of DR plan		
Service Level ID	18		
Definition	Once per year activity to test DR preparedness		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Test Completion	Annual test of the DR plan completed and accepted by County in accordance with the criteria agreed upon by County and Contractor prior to execution of each annual test	100%	No earnback provision
Formula	Number of instances within Performance Target/Total number of instances during Measurement Period		
Measurement Period	Once		
Reporting Period	Annual		
Measurement Tool/Source Data	Contractor DR Test Report		

6.12 Application Recovery Post-Disaster

Service Level	Recovery of Applications following disaster		
Service Level ID	19		
Definition	Recovery of applications after a disaster		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Application Recovery	P1 Apps — 48 hours with ≤28 hours of data loss P2 Apps — 72 hours with ≤28 hours of data loss	100%	No earnback provision
Formula	Number of instances within Performance Target/total number of instances during Measurement Interval		
Measurement Interval	Designated recovery period following a disaster		
Reporting Period	Periodically throughout the recovery period		
Measurement Tool/Source Data	Contractor-provided		

6.13 Asset Tracking

Service Level	Management of Assets		
Service Level ID	20		
Definition	Effective management of Assets		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Accurate tracking of Asset components	Accuracy of serial numbers, assigned Location/Person, Hardware/Software configuration	99%	99.5%
Formula	This SL is a comparison of 8 fields as discovered via SCCM (EUS assets), DDMi (Datacenter Assets), scripts (Storage assets) and Spectrum (AT&T Network assets) in a given month versus the data for those assets as found in Asset Manager 9 (AM9). Asset types measured will be all Desktop, Workstation, Laptop, Windows Tablet, Server, Storage, and Network. Attributes that will used to measure this SL: 1. Device Name 2. Serial Number 3. Brand 4. Model 5. Location (CoSD Site Level) 6. Status (Deployed) 7. OS (EUS and Servers) 8. Owner Login ID (EUS) The denominator will be the (number of assets auto-discovered in a given month) * (number of fields), with location only gathered for Desktops, Workstations, Laptops, and Windows Tablets. The numerator will be the (number of fields that matched between AssetManager and autodiscovery) Example Calculation: 15,000 Assets discovered in month. Of those, there were 200 fields that failed. (15000*8)-200 / (15000*8) = 99.83% Matching will be done based on Computer Name. Location (not a discoverable field) will be scored based on County issued ITrack location disputes which are deemed valid, after confirming an IMAR or ITrack CR had been submitted and not properly executed. Owner Login ID will be scored based on County issued ITrack Owner Login ID disputes which are		

	deemed valid, after confirming an IMAR or ITrack CR had been submitted and not properly executed.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	System provided by the Contractor to track and report out-of-compliance activities

6.14 Root Cause Analysis

Service Level	Root Cause Analysis conducted on critical incidents		
Service Level ID	21		
Definition	Assessment of Problems and their causes, with resolutions		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Elapsed Time to produce RCA report	7 business days from S1 and S2 Incidents or other Incidents as requested by County starting at Incident Resolution	99%	99.5%
Formula	Number of instances within Performance Target/total number of instances during Measurement Interval Note – completion criteria for publication of RCA shall be per the identified process in the Standards and Procedures manual		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Measured by the Ticket management system		

6.15 Key Personnel Vacant Position

Service Level	Filling vacant Key Personnel positions		
Service Level ID	22		
Definition	Duration a Key Position is vacant beyond required timeframe to fill		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Number of days position is vacant	2 business day after Key Position becomes vacant	100%	No earnback provision
Formula	Vacant Key Positions filled within the target/all vacant Key Positions filled		
Measurement Interval	Daily		
Reporting Period	Monthly		
Measurement Tool/Source Data	Formal notification in writing of the individual filling the position. If the individual is an interim, a target date for the permanent assignment shall be provided.		

7 SERVICE DESK SERVICE LEVELS

7.1 Incident Resolution Confirmation Notice

Service Level	Providing a Resolution Confirmation notice for all Incident tickets and Service Requests		
Service Level ID	23		
Definition	Total time elapsed to provide all resolution confirmation notices via automated email notification and/or telephone call to the End-User. Service Desk may leave a message with a phone number to call back with any questions. For Incident Tickets, if a message is left, the Incident Ticket shall remain open in a pending closure status for 24 hours to allow the End-User the opportunity to confirm the incident is Resolved.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Schedule	Confirmation Notice within 30 minutes of Incident resolution	99%	99.5%
Formula	Number of instances within Performance Target/Total number of instances during Measurement Interval		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Recording the confirmation notice received in the Ticket management system		

7.2 Password Reset Completion

Service Level	Length of time between password reset request and completion		
Service Level ID	24		
Definition	All requests		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Schedule	• 30 minutes • 60 minutes	• 95% within 30 minutes • 99% within 60 minutes	• 97.5% within 30 minutes • 99.5% within 60 minutes
Formula	Number of instances within Performance Target/total number of instances during Measurement Interval		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Recording the request completion in the Ticket Management System		

7.3 Response Time

Service Level	Response Time for: • Speed-to-answer • Call abandonment rate • Email Response Time • Voice Mail Response Time		
Service Level ID	25		
Definition	Response Time is the duration (measured in seconds) the End-User requires to connect with the Contractor's contact center representative. The Contractor will provide toll-free telephone lines in sufficient quantity to handle the call volume; ACD system(s) to record call date, time and duration information; and electronic interfaces to all systems for monitoring and reporting.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**

• A. Speed-to-answer Time	• ≤ 75 seconds beginning 1st full month of 1st year of measurement in effect; 65 seconds for 2nd year of measurement in effect; 55 seconds for 3rd year of measurement in effect; 45 seconds for 4th year + of measurement in effect	• 90%	• 95%
• B. Speed-to-answer Time	• ≤ 90seconds	• 99%	• 99.5%
• Call abandonment rate	• ≤5%	• 100%	• Same formula, but performance target modified to 2.5%
• Online Response Time	• ≤1 hour	• 95%	• 97.5%
• Voice Mail Response Time	• ≤30 minutes	• 95%	• 97.5%
Formula	Number of instances within Performance Target divided by Total number of instances during Measurement Interval All Respond Time metrics must be met for this Respond Time Service Level. However, if Call Abandonment rate is 4% or less then B. Speed-to-answer Time is considered met for the current month.		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor-provided		

7.4 Service Repair Scheduling

Service Level	The amount of time necessary to schedule a Service Repair		
Service Level ID	26		
Definition	The elapsed time from the time the call is determined to be a desktop Incident Ticket until the End-User is contacted to schedule an onsite service appointment.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Time to complete scheduling	Within 90 minutes	98%	99%
Formula	Number of instances within Performance Target/Total number of instances during Measurement Interval		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Desktop Incident resolution Tickets only		

7.5 Customer Satisfaction

Service Level	Customer Satisfaction after Service performance		
Service Level ID	27		
Definition	Measures the performance of the Service provided to End-User		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Positive Evaluation Percentage	Percentage of Positive Survey Evaluations (Score 3 and 4)	▪ Year 1 (May 2022 - April 2023) ≥ 90.0% Year 2 and onward (May 2023 – onward) ≥ 91.0%	94%
Formula	Percentage of Positive Survey Evaluations = Total number of survey evaluations returned scoring 3 and 4 divided by Total number of surveys returned. Surveys will be rated on the following four (4) point scale: 1 – Highly Dissatisfied, 2 – Dissatisfied, 3 – Satisfied, 4 – Highly Satisfied. Internal Contractor tickets will be excluded from the survey population. Contractor shall calculate SL performance based on a statistically valid sample which is defined as a 95% confidence level with a 5% margin of error, .5% standard deviation, using a mutually agreed calculator found in the public domain: https://www.qualtrics.com/experience-management/research/determine-sample-size/. If there is insufficient number of surveys returned for a statistically valid sample for a given month, the low volume condition provision as per Section 2.10 – Low Volume Conditions, of Schedule 16.8 – Fee Reductions applies.		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Survey data, ServiceNow		

7.6 First Call Resolution

Service Level	Resolution on first call		
Service Level ID	28		
Definition	First call resolution applies when an end-user request or issue is resolved prior to the conclusion of the call or chat with the Service Desk.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent completed	Call resolved	66%	75%
Formula	Number of tickets closed and resolved on first call or chat/total number of calls and chats during Measurement Interval.		
Measurement Interval	Daily		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor provides a system with date and time stamp capabilities to track and report out-of-compliance activities.		

7.7 First Call Resolution – 2nd Generation

Service Level	Resolution on first call		
Service Level ID	54		
Definition	First call resolution applies when an end-user request or issue is resolved prior to the conclusion of the call or chat to include hot hand-offs to support tiers other than Service Desk. On implementation of end user enablement projects (e.g. self-service or self-help projects), the parties shall mutually agree this SL shall receive 0% weighting for a duration of 6 months (or as mutually agreed); after the six months, the parties shall either validate the current performance target or mutually agree on a revised performance target.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent completed	Call resolved	70%	No earnback provision
Formula	Number of tickets closed and resolved on first call (continuous call) or chat/total number of calls and chats during Measurement Interval		
Measurement Interval	Daily		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor provides a system with date and time stamp capabilities to track and report out-of-compliance activities. (Service Manager, chat, SSPR tool).		

8 END-USER SERVICE LEVELS

8.1 Critical Software Patches

Service Level	Operating System (OS) / Microsoft Office patches involving technical issues and security vulnerabilities		
Service Level ID	29-1		
Definition	Implementation of OS patches and updates for desktop computing assets.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Time to Implement	Measured from the approved mandatory installation deadline which must occur within the timeline respective to the update/patch highest severity rating, per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If the highest severity rating is high, the patch must be deployed within 30 days of the patch release date. If the patch/update is made available on November 1st, the approved mandatory installation must commence before December 1st. If the approved mandatory installation deadline is November 15th, the SLA must be met by December 15th.	93% all PCs	96.5% all PCs

Formula	Qty of workstations patched/updated over patch cycle period ÷ (Qty of workstations in the environment - Qty of Unknown workstations - Qty of Exempt workstations) Unknown workstations are those that have not connected to the County network for an extended period (at least 90 days) and have not accepted the deployment. Exempt workstations are those that have been approved and documented as exempt. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).
Measurement Interval	Monthly based on Patch Cycle, not on the calendar month.
Reporting Period	Monthly based on Patch Cycle Initial Report - delivered 7 days prior to completion of the Patch Cycle period Final Report - delivered within 72 hours after Patch Cycle period
Measurement Tool/Source Data	Contractor-provided

Service Level	Operating System (OS) and Core Software patching for Critical and Zero Day Vulnerabilities		
Service Level ID	29-2		
Definition	Implementation of Core Software and OS patches and updates specifically identified as Critical or Zero Day Vulnerabilities. Core Software is defined in Schedule 5, Report 64.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Time to Implement	Measured from the approved mandatory installation deadline which must occur within 15 calendar days as defined per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If the severity rating is Critical, the patch must be deployed within 15 days. If the patch/update is made available on November	93% all PCs	96.5% all PCs

	1st, the approved mandatory installation must commence before November 15th. If the approved mandatory installation deadline is November 5th, the SLA must be met by November 20th.		
Formula	Qty of workstations patched/updated over patch cycle period ÷ (Qty of workstations in the environment - Qty of Unknown workstations - Qty of Exempt workstations). Unknown workstations (at least 90 days) are those that have not connected to the County network for an extended period and have not accepted the deployment. Exempt workstations are those that have been approved and documented as exempt. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).		
Measurement Interval	As needed based on Critical and Zero Day Vulnerabilities produced with vendor remedy.		
Reporting Period	Initial Report - delivered on day 9 from patch availability from the vendor Final Report - delivered within 72 hours after Patch Cycle period		
Measurement Tool/Source Data	Contractor-provided		

Service Level	Core Software patching involving technical issues and security vulnerabilities		
Service Level ID	29-3		
Definition	Implementation of Core Software patches for desktop computing assets. Core Software is defined in Schedule 5, Report 64.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Time to Implement	Measured from the approved mandatory installation deadline which must occur within the timeline respective to the update/patch highest severity rating, per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If the highest severity rating is high, the patch must be deployed within 30 days of	93% all PCs	96.5% all PCs

	the patch release date. If the patch/update is made available on November 1st, the approved mandatory installation must commence before December 1st. If the approved mandatory installation deadline is November 15th, the SLA must be met by December 15th.		
Formula	(Qty of workstations patched/updated over patch cycle period + Qty of in progress workstations patched/updated over patch cycle period) ÷ (Qty of workstations in the environment – Qty of Unknown workstations – Qty of Exempt workstations). In Progress workstations are those that have received the deployment, but the user has not taken the necessary action for the install to complete. Unknown workstations are those that have not connected to the County network for an extended period (at least 90 days) and have not accepted the deployment. Exempt workstations are those that have been approved and documented as exempt. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).		
Measurement Interval	Monthly based on Patch Cycle, not on the calendar month.		
Reporting Period	As Core Patches are Released. Initial Report - delivered 7 days prior to completion of the Patch Cycle period Final Report - delivered within 72 hours after Patch Cycle period		
Measurement Tool/Source Data	Contractor-provided		

8.2 Software IMAR

Service Level	Completion of Software IMAR		
Service Level ID	30		
Definition	Acceptable time required to Install, Move, Add or Remove Software at a desktop upon County authorization of Service Request (SR) for items covered in the Optional Items Catalogue (OIC).		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Elapsed Time	30a) 2 business days after an add SR is authorized by County or by requested date in SR or date scheduled by Contractor and accepted by requestor when software license is available at time of SR	30a) 90%	30a) 95%
	30b) 7 business days after an add SR is authorized by County or by requested date in SR or date scheduled by Contractor (based on vendor delivery date) and accepted by requestor if software license is not available at the time of the SR	30b) 90%	30b) 95%
	30c) 3 business days after a move or remove SR is authorized by County or by requested date in SR or date scheduled by Contractor and accepted by requestor Business Day Monday — Friday 6 a.m. to 6 p.m., excluding the County Holidays	30c) 90%	30c) 95%

Formula	Number of instances within Performance Target/Total number of instances during Measurement Interval. User requests that specify IMAR execution will be measured from the point of the scheduled time. 30a) Number of requests completed within 2 business days or by requested date in SR or date scheduled by Contractor and accepted by requestor (when software license is available) divided by number of requests completed (when software license is available) >= 90% 30b) Number of requests completed within 7 business days or by requested date in SR or date scheduled by Contractor and accepted by requestor (when software license is not available) divided by number of requests completed (when software license is not available) >= 90% 30c) Number of software move/remove requests completed within 3 business days or by requested date in SR or date scheduled by Contractor and accepted by requestor divided by number of software move/remove requests completed >= 90% For clarity 30a, 30b, and 30c must be met for this Service Level. Clock will be suspended if County approval is required.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Contractor-provided

8.3 Hardware IMAR

Service Level	Completion of Hardware IMAR		
Service Level ID	31		
Definition	Acceptable time required to Install, Move, Add or Remove Hardware upon County authorization of Service Request (SR). This applies to End User Resource Unit hardware such as desktop computing devices, network printers, and telephones.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Elapsed Time	31a) 3 business days after an add or install SR is authorized by County or by requested date in SR or date scheduled by Contractor and accepted by requestor when hardware is available at time of SR	31a) 90%	31a) 95%
	31b) 7 business days after an add or install SR is authorized by County or by requested date in SR or date scheduled by Contractor (based on vendor delivery date) and accepted by requestor if hardware is not available at the time of the SR	31b) 90%	31b) 95%
	31c) 3 business days after a move or remove SR is authorized by County or by requested date in SR or date scheduled by Contractor and accepted by requestor Business Day Monday — Friday 6 a.m. to 6 p.m., excluding the County Holidays	31c) 90%	31c) 95%

Formula	Number of instances within Performance Target/Total Number of instances during Measurement Interval. Service Requests that specify IMAR execution will be measured from the point of the scheduled time. 31a) Number of requests completed within 3 business days or by requested date in SR or date scheduled by Contractor and accepted by requestor (when hardware is available) divided by number of requests completed (when hardware is available) >= 90% 31b) Number of requests completed within 7 business days or by requested date in SR or date scheduled by Contractor and accepted by requestor (when hardware is not available) divided by number of requests completed (when hardware is not available) >= 90% 31c) Number of hardware move/remove requests completed within 3 business days or by requested date in SR or date scheduled by Contractor and accepted by requestor divided by number of hardware move/remove requests completed >= 90% For clarity, 31a, 31b, and 31c must be met for this Service Level. Clock may only be suspended if County approval is required.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Contractor-provided

8.4 OIC Additions, Updates and Removals

Service Level	Completion of addition, update, or removal request pertaining to Optional Items Catalog (OIC)		
Service Level ID	32		
Definition	The elapsed time between Catalog Review Board (CRB) approval of Service Request (SR) to add, remove or update item to or from the OIC and completion of the SR with completion defined as when OIC is updated with addition, removal, or update of item.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Elapsed time	30 Days	80%	90%
Formula	Number of instances within Performance Target/Total number of instances during Measurement Interval		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor-provided		

9 NETWORK SERVICE LEVELS

9.1 Transaction Response Time — Internet/Intranet Access

Service Level	Internet/Intranet systems. Response is measured from each Site		
Service Level ID	33		
Definition	Length of time host systems and networks transmit and process requests across the Internet/Intranet and return data to End-User's screen. Internet/ Intranet Respond Time will be measured by accessing the County Internet/ Intranet Sites		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Response Time	Intranet – Within 0.5 seconds Internet – Within 0.75	98% 98%	99% 99%
Formula	1. Test transactions will be sent to designated County endpoints for Intranet/Internet locations every 15 minutes. 2. These transactions will be tested 6 a.m. to 6 p.m. M-F, excluding County Holidays. 3. The algorithm shall be: Number of Internet/Intranet transactions per hour (4) x number of hours checked per day (12) x number of days per Month. 4. The percentage is derived from the number of passing transactions/number of possible transactions		
Measurement Interval	Every 15 minutes		
Reporting Period	Monthly		
Measurement Tool/Source Data	Time is measured using a defined sampling scheme, data transfer sizes and network Locations. The current measurement tool is network probes, replaced by APM after deployment		

9.2 Transaction Response Time – Data Center

Service Level	Transaction Response Time for Server Systems — Local Network		
Service Level ID	34		
Definition	Length of time host systems and networks transmit and process requests and return data to End-User's screen. Response Time will be measured using a defined sampling scheme, data transfer sizes and network Locations. County Sites and management of the probes used will be documented in the Standards and Procedures Manual.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Response Time	24/7	• 95% within 1 seconds • 99% within 3 seconds	• 97.5% • 99.5%
Formula	1. Test transactions will be sent to an endpoint selected at random. This will be repeated 100 times, and the average response time of the 100 transactions will be recorded. 2. Step 1 will be repeated twice a day, at 9 a.m. and 10 a.m. as well as 2 p.m. and 3 p.m., two days a Week, on chosen business days at random. 3. At the conclusion of the calendar Month, the recorded data for all samples will be added together, divided by the number of samples, and reported.		
Measurement Interval	See formula		
Reporting Period	Monthly		
Measurement Tool/Source Data	Time is measured using a defined sampling scheme, data transfer sizes and network Locations. The current measurement tool is network probes, replaced by APM after deployment		

9.3 Voice System Call Blocking

Service Level	Voice system call blocking		
Service Level ID	35		
Definition	Percentage of calls blocked, or experiencing busy service, measured per trunk route		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Calls blocked	24/7	Blocking not to exceed 1% of all calls during each hour by route unless otherwise directed by the County	Not to exceed 0.5% of all calls during each hour by route unless otherwise directed by the County
Formula	Number of calls blocked or experiencing busy service each hour per trunk/total calls attempted per hour per trunk. This metric will be calculated for each hour of the Month for each phone switch.		
Measurement Interval	Hourly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

9.4 Data Network Availability

Service Level	The percentage of time that the data network is available.		
Service Level ID	36a, 36b, 36c		
Definition	The time during which the network is fully functioning and normal business operations can be carried out with no data loss, downtime, or performance degradation during available site hours.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	**36a:** D1 = average availability of all network circuits and active components	D1 ≥ 99.95% aggregate availability	D1: ≥ 99.975%
	36b: D2 = Individual site connected via fiber with the lowest availability	D2 ≥ 99.5% per fiber Site availability	D2: ≥ 99.75%
	36c: D3 = Individual site connected via copper with the lowest availability	D3 ≥ 99% per copper Site availability	D3: ≥ 99.5%
Formula	**36A** Components include all circuits and active data network components Component Availability (%) = 100% - Component Unavailability (%) Component Unavailability = Component outage duration / Available Component Hours Component outage duration does not include scheduled outages 36A = if Average Component Availability of All Active Components >= 99.95%, then Pass; otherwise, Fail. **36B & 36C** Site availability (%) = 100% - Site Unavailability Site Unavailability = Total Outages at Site / Site Available Hours Outages do not include scheduled outages 36B= If Site Availability for all Sites linked via fiber >= 99.5%, then Pass; otherwise, see credit table 4.8.14. 36C = If Site Availability for all Sites linked via copper >= 99%, then Pass; otherwise, see credit table 4.8.14.		

Measurement Interval	Monitor Continuously/Measure Daily
Reporting Period	Monthly
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data. All performance criteria are to be measured on a per circuit and component basis.

9.5 Internet Availability

Service Level	The availability of the Internet. The percentage of time that the Internet is available for normal business operations.		
Service Level ID	37		
Definition	Percentage of time Internet access is available		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	24/7	99.80%	99.9%
Formula	Availability (%) = 100% — Unavailability (%) Where Unavailability is defined as: (Sum of Outage Duration x 100%) / (Schedule Time — Planned Outage)		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

9.6 Voice Network Availability

Service Level	The percentage of time that the Voice Services (telephone, PBX or voice mail) is available for normal business operations		
Service Level ID	38		
Definition	Percentage of time that the Voice Services are available for use		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	24/7	99.80%	99.9%
Formula	Availability (%) = 100% — Unavailability (%) Where Unavailability is defined as: (Sum of Outage Duration x 100%)/(Schedule Time — Planned Outage)		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

10 DATA CENTER SERVICE LEVELS

10.1 Output Delivery

Service Level	Delivery of printed output		
Service Level ID	39		
Definition	Percentage of time that the printed output is created and delivered on time and free from errors and omissions		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Percent Attained	Per County schedule Monday — Friday 6 a.m. to 6 p.m., excluding the County Holidays	98%	99%
Formula	Number of times output met the print window for delivery/total output deliveries		
Measurement Interval	Daily		
Reporting Period	Monthly		
Measurement Tool/Source Data	The tool supplied by the Contractor automatically records date and time stamps each activity within a process, including uptime and downtime data		

10.2 Daily Backup

Service Level	Daily Backup for: • Incremental • Full		
Service Level ID	40		
Definition	Backup of files that have changed or are new since the last daily backup including a full backup once a week		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Backup complete	Monthly	99.95	No Earnback
Formula	Daily: Number of objects successfully backed up within Measurement Interval divided by Ttotal number of objects within Measurement Interval Monthly: Number of objects successfully backed up within the month divided by Total number of objects for the month		
Measurement Interval	Daily and Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	The tool supplied by the Contractor automatically records date and time stamps each activity within a process. Contractor shall create a Severity 2 Incident ticket in every event which an object failed to be backed up for two consecutive days. Note: Objects can be a UNIX Filesystem, Windows Volume, a Windows or UNIX folder, NetApp or NAS shares/directories, VMWare server image or OS Volume.		

10.3 Quarterly Backup / Restore

Service Level	Addresses any gaps in proper operation of backup and restore		
Service Level ID	41		
Definition	Confirmation that the backup and restore is properly operating		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Successful test completion	Test completed and confirmed	100%	No earnback provision
Formula	Successful test completion		
Measurement Interval	Monthly		
Reporting Period	Quarterly		
Measurement Tool/Source Data	Contractor-provided		

10.4 Data Restore

Service Level	Data restore measurements: • Restore Service Request for production data • Restore Service Request for recovery of test data or data volume backups		
Service Level ID	42		
Definition	Initiation of restore Service Request		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
a. Respond Time data 30 days old or less b. Respond Time data 31 days old or more	a. ≤3 hours from Service Request submittal b. ≤8 hours from Service Request submittal	a. 95% b. 95%	a. 97.5% b. 97.5%
Formula	Restore initiation within the required timeframes, SL success requires meeting performance targets on both a AND b.		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor-provided		

10.5 Server Decommission

Service Level	Completion of decommission request		
Service Level ID	43		
Definition	Removal of either a physical or a virtual Server from active status and from active billing, if applicable		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Completion Time	Server decommission Monday — Friday 6 a.m. to 6 p.m., excluding the County Holidays	• 95% within 3 business days • 100% within 30 business days	• 97.5% within 3 business days • No earnback provision
Formula	Number of Servers decommissioned within target/total number of Servers authorized for removal during Measurement Interval		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor-provided		

10.6 Server Provisioning

Service Level	Server Provisioning		
Service Level ID	44		
Definition	Provisioning a physical production or test Server for use in the network following date of Solution Design Document (SDD) approval. Note: Server provisioning is defined as Operating System is installed, and tools (as defined in the Build Docs) are installed for management, monitoring, backups and anti-virus, network configuration and on-line, and project team has access and authorization in-place.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Completion	• **44-a Physical (excluding Oracle):** within 40 business days from SDD approval	• 95%	• 97.5%
	• **44-b Virtual:** within 8 business days from SDD approval	• 95%	• 97.5%
	• **44-a Physical (Oracle):** within 59 business days from SDD approval	• 95%	• 97.5%
Formula	• **44-a** Number of Servers Requested for Provisioning within Performance Target / Total Number of Servers Requested • **44-b** Number of Servers Requested for Provisioning within Performance Target / Total Number of Servers Requested • **44-c** Number of Servers Requested for Provisioning within Performance Target / Total Number of Servers Requested Business Day: Monday - Friday 6 a.m. to 6 p.m., excluding the County Holidays		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Contractor-provided		

10.7 [Reserved]

10.8 [Reserved]

10.9 [Reserved]

10.10 [Reserved]

10.11 Server Software Update

Service Level	Operating System Patching for Windows and Linux servers		
Service Level ID	46-1		
Definition	Implementation of operating system patches and updates for Windows and Linux servers		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Time to Implement	Within the Patch Cycle, starting on the day after Patch Tuesday of current month, when patches and updates made available from Microsoft and RedHat, through Monday before Patch Tuesday of the next month. Example: If Patch Tuesday for November is November 9th and Patch Tuesday for December is December 14th, the patch cycle for the period is November 10th through December 9th. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).	95%	97%
Formula	Quantity of Windows and Linux servers patched/updated over patch cycle divided by the Quantity of Windows and Linux servers in the environment (less approved exceptions).		
Measurement Interval	Monthly based on Patch Cycle, not the calendar month.		
Reporting Period	Monthly based on Patch Cycle, delivered on the Wednesday after completion of the Patch Cycle. Example: If Patch Tuesday for November is November 9th and Patch Tuesday for December is December 14th, the patch cycle for the period is November 10th through December 9th. Report delivery date December 15th.		
Measurement Tool/Source Data	Contractor-provided (Ansible)		

Service Level	Operating System Patching for Solaris and AIX servers
Service Level ID	46-2

Definition	Implementation of operating system patches and updates for Solaris and AIX servers.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Time to Implement	Within the Patch Cycle, starting on the day after Patch Tuesday of current month, through Monday before Patch Tuesday of the next month. Oracle and IBM release patches on a quarterly basis, not monthly. Example: If Patch Tuesday for January is January 11th and Patch Tuesday for February is February 8th, the patch cycle for the period is January 12th through February 7th. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).	95%	97%
Formula	Quantity of Solaris and AIX servers patched/updated over patch cycle divided by the Quantity of Solaris and AIX servers in the environment (less approved exceptions).		
Measurement Interval	Quarterly based on Patch Cycle, not on the calendar month.		
Reporting Period	Quarterly based on Patch Cycle, delivered on the Wednesday after completion of the Patch Cycle. Example: If Patch Tuesday for January is January 11th and Patch Tuesday for February is February 8th, the patch cycle for the period is January 12th through February 7th. Report delivery date February 9th.		
Measurement Tool/Source Data	Contractor-provided (Ansible)		

Service Level	Operating System Patching for Critical and Zero Day Vulnerabilities
Service Level ID	46-3
Definition	Implementation of operating system (Linux, Windows, Solaris and AIX) patches and updates specifically identified as Critical or Zero Day Vulnerabilities

Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to Implement	Within 24 hours of patches or updates being made available from operating system vendor(s) and 98% within 72 hours. A client approved Emergency Change Request is required pre-deployment or post-deployment Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).	92%	95%
Formula	Quantity of servers patched/updated divided by Quantity of servers impacted by the Critical or Zero Day Vulnerability in the environment (less approved exceptions).		
Measurement Interval	As needed based on Critical and Zero Day Vulnerabilities produced with vendor remedy.		
Reporting Period	As needed but within 24 hours of implemented patches and updates for Critical or Zero Day Vulnerabilities for initial report and within 96 hours for the final report.		
Measurement Tool/Source Data	Contractor-provided		

Service Level	Middleware Vulnerability Remediation for Production PAIDs		
Service Level ID	46-4		
Definition	Remediation of 'critical' and 'high' vulnerabilities found in middleware software that support production applications.		
Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to implement	Within the rolling 60-day Remediation Cycle (RC), starting on the first day of month and last day of following month (generally 60 days). SL report and exceptions report shall be delivered on the 14th of the month immediately following completion of the RC.	80%	90%

	Example: If RC #1 period is June 1st through July 31st with reporting due August, then RC #2 period is July 1st through August 31st with reporting due September and so on. Example timeline: • Vulnerability scan execution – June 1st • RC #1 period start – June 1st • Vulnerability scan execution – July 1st • RC #2 period start – July 1st • RC #1 period end – July 31st • Vulnerability scan execution – August 1st • RC #3 period start – August 1st • Delivery of report for cycle #1 – August 14th • RC #2 period end – August 31st • Vulnerability scan execution – September 1st • Delivery of report for cycle #2 – September 14th • RC #3 period end – September 30th • Vulnerability scan execution – October 1st • Delivery of report for cycle #3 – October 16th Acceptable exceptions are limited to: • Preventing disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April); Employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze; etc.). • Current application version not certified for update of middleware. • Significant upgrade project in progress for PAID will be impacted. Vulnerability remediation shall be applied to development, test, and production environments. Vulnerabilities are identified in the vulnerability scan data provided by the ITO Security team. Though scanning is done more often, the scan data used for this SL will be		

	from the scans executed on the 1st of the month of the appropriate remediation period months.		
Formula	Quantity of in-scope "critical" and "high" middleware vulnerabilities (as identified in the vulnerability scan data) remediated during the RC **divided by** Quantity of in-scope "critical" and "high" middleware vulnerabilities (as identified in the vulnerability scan data) at the beginning of the RC. "In-scope" quantity excludes acceptable exceptions. "Remediated during the RC" is calculated by comparing the in-scope vulnerability scan results from the end of the current RC to the in-scope vulnerability scan results from the beginning of the current RC. Any in scope vulnerabilities from the beginning of the RC that is no longer evidenced at end of the RC data, is considered "remediated". For example, for the RC period June 1st through July 31st, formula calculation is as follows: (Quantity of "critical" and "high" middleware vulnerabilities remediated d June RC) ——————— **divided by**——————— (Quantity of in-scope "critical" and "high" middleware vulnerabilities on Ju Furthermore, for the subsequent RC period July 1st through August 31st, formula calculation is as follows: (Quantity of "critical" and "high" middleware vulnerabilities remediated d July RC) ——————— **divided by**——————— (Quantity of in-scope "critical" and "high" middleware vulnerabilities on Ju		
Measurement Interval	Monthly, based on rolling 60-day RC.		
Reporting Period	Bi-monthly (every two months), based on RC, delivered on the 14th of the month after completion of the RC. The exceptions report will also be delivered on the 14th of the month after completion of the RC. If the 14th of the month is a weekend or holiday, the report will be provided on the next business day. Example: For the RC period June 1st through July 31st, the SL and exceptions reports shall be delivered on August 14th. For the subsequent RC period July 1st through August 31st, the SL and exceptions reports shall be September 14th, and so on.		
Measurement Tool/Source Data	Contractor-provided		

Service Level	Application Vulnerability Remediation for Production PAIDs		
Service Level ID	46-5		
Definition	Remediation of 'critical' and 'high' vulnerabilities found at the application level for production applications.		
Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to Implement	Within the rolling 60-day Remediation Cycle (RC), starting on the first day of month and last day of following month (generally 60 days). SL report and exceptions report shall be delivered on the 14th of the month immediately following completion of the RC. Example: If RC #1 period is June 1st through July 31st with reporting due August, then RC #2 period is July 1st through August 31st with reporting due September and so on. Example timeline: • Vulnerability scan execution – June 1st • RC #1 period start – June 1st • Vulnerability scan execution – July 1st • RC #2 period start – July 1st • RC #1 period end – July 31st • Vulnerability scan execution – August 1st • RC #3 period start – August 1st • Delivery of report for cycle #1 – August 14th • RC #2 period end – August 31st • Vulnerability scan execution – September 1st • Delivery of report for cycle #2 – September 14th • RC #3 period end – September 30th • Vulnerability scan execution – October 1st • Delivery of report for cycle #3 – October 16th Acceptable exceptions are limited to: • Preventing disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; Employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze; etc.). • Vulnerability remediation requires an application upgrade. • Significant upgrade project in progress for PAID will be impacted. Vulnerability remediation shall be applied to development, test, and production environments.	80%	90%

	Vulnerabilities are identified in the vulnerability scan data provided by the ITO Security team. Though scanning is done more often, the scan data used for this service level will be from the scans executed on the 1st of the month of the appropriate remediation period months.		
Formula	Quantity of in-scope "critical" and "high" application vulnerabilities (as identified in the vulnerability scan data) remediated during the RC **divided by** Quantity of in-scope "critical" and "high" application vulnerabilities (as identified in the vulnerability scan data) at the beginning of the RC. "In-scope" quantity excludes acceptable exceptions. "Remediated during the RC" is calculated by comparing the in-scope vulnerability scan results from the end of the current RC to the in-scope vulnerability scan results from the beginning of the current RC. Any in scope vulnerabilities from the beginning of the RC that is no longer evidenced at end of the RC data, is considered "remediated". For example, for the RC period June 1st through July 31st, formula calculation is as follows: (Quantity of "critical" and "high" application vulnerabilities remediated during the June RC) **divided by** (Quantity of in-scope "critical" and "high" application vulnerabilities on June 1st scan) Furthermore, for the subsequent RC period July 1st through August 31st, formula calculation is as follows: (Quantity of "critical" and "high" application vulnerabilities remediated during the July RC) **divided by** (Quantity of in-scope "critical" and "high" application vulnerabilities on July 1st scan)		
Measurement Interval	Monthly, based on rolling 60-day RC.		
Reporting Period	Bi-monthly (every two months), based on RC, delivered on the 14th of the month after completion of the RC. The exceptions report will also be delivered on the 14th of the month after completion of the RC. If the 14th of the month is a weekend or holiday, the report will be provided on the next business day. Example: For the RC period June 1st through July 31st, the SL and exceptions reports shall be delivered on August 14th. For the subsequent RC period July 1st through August 31st, the SL and exceptions reports shall be September 14th, and so on.		
Measurement Tool/Source Data	Contractor-provided		

10.12 Server Availability

<table>
<tr><td>Service Level</td><td colspan="3">The percentage of time that the server is available</td></tr>
<tr><td>Service Level ID</td><td colspan="3">47</td></tr>
<tr><td>Definition</td><td colspan="3">The percentage of time that the system is available for business operations.</td></tr>
<tr><td>Service Measure</td><td>Performance Target</td><td>SL Performance (%)</td><td>SL Earnback</td></tr>
<tr><td>Availability</td><td>24/7</td><td>99.5% - 99.8% per production Server per Step Reduction Schedule Table
95% per test Server
95% per utility Server</td><td>99.9% per production Server

97.5% per test Server
97.5% per utility Server</td></tr>
<tr><td>Formula</td><td colspan="3">Availability (%) = 100% — Unavailability (%)
Where Unavailability is defined as: (Sum of Outage Duration x 100%)/((Schedule Time — (Planned Outage))

Use the Step Reduction Schedule Table to determine the applicable Fee Reduction percentage and subsequently calculate the Fee Reduction amount for a given month. Determine the Fee Reduction percentage based on sum total of Servers that missed the SL Performance and 6-month interval in which given month occurs. For example, in January 2021, four servers missed the SL Performance. Since January 2021 is in the ‘Months 7-12’ interval, a 25% Fee Reduction percentage applies for calculating the Fee Reduction amount.

Step Reduction Schedule Table
<table>
<tr><th>Step</th><th>Sum Total of Servers that Missed SL Performance</th><th>*Months 1-6 Fee Reduction 99.5% per Production Server</th><th>**Months 7-12 Fee Reduction 99.8% per Production Server</th><th>***Months 13+ Fee Reduction 99.8% per Production Server</th></tr>
<tr><td>0</td><td>0 to 3</td><td>0%</td><td>0%</td><td>25%****</td></tr>
<tr><td>1</td><td>4 to 6</td><td>25%</td><td>25%</td><td>50%</td></tr>
<tr><td>2</td><td>7 to 9</td><td>50%</td><td>50%</td><td>75%</td></tr>
<tr><td>3</td><td>10+</td><td>100%</td><td>100%</td><td>100%</td></tr>
</table>
</td></tr>
</table>

	*July – December 2020 ** January – June 2021 *** July 2021 and after **** One server miss at 0%, 2 or 3 server miss are at 25% For clarity, unplanned outage time shall not be accrued if the server is part of a high availability system/cluster, where the service provided by the server system/cluster remains available. Utility Servers exist in the environment to optimize support capabilities. No County traffic passes through these servers and they have no direct impact on access, availability, or performance of County users or data. Utility Servers provide: • Redundant Accessibility • Administration of Services • Administration of Cyber Security and Compliance • Command Line Interfaces for Administration of ESXi As of 08/10/2020, there are nine utility servers: USSDSCOSD780, USSDSCOSD781, USPLSCOSD105, USTLSCOSD105, USSDGACSD0001, USTLPACSD0001, USPLVUCSD025, USTLVUCSD050, and USTLPOCSD0012.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data

11 APPLICATIONS SERVICE LEVELS

11.1 Project Management Plan Rework

Service Level	Each Project Management Plan (PMP) rejection that requires revision, and: a) the revision is delivered during the Measurement Period; and b) the rationale for rejection is either due solely to Contractor-related issues, or a combination of Contractor and County issues		
Service Level ID	48		
Definition	Project delay in Business Hours due to Rejection and Revision of PMP. The number of Business Hours delayed is defined as the number of business hours from the County's notification date to Contractor of a PMP rejection through, and including, the County's receipt of Contractor's revised PMP. As a part of the rejection process, the County will identify the category that the rejection falls within, as well as the specific rejection reason. 1. Contractor Caused Reasons for Rejection (SL clock starts) must be categorized as: A. Project scope is incorrect based on county input document provided B. Contractor Math error C. Contractor Schedule issue D. Contractor Fees applied incorrectly E. Changes made after "draft" review 2. County Caused Reasons for Rejection (SL clock does not start) must be categorized as: A. County requested changes to scope B. County requested changes to list of planned work products to be delivered C. PMP timeframe for approval has expired D. County requested changes to business requirements E. Time is lost solely due to contract disputes/reasons		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Schedule	Number of Business Hours delayed during Measurement Period ≤Target Baseline Total of County Business Hours delayed	The Target Baseline Total of Business Hours delayed is • 102 hours	No Earnback provision

Formula	Average Number of County Business Hours Delayed = sum of County Business Hours Delayed on each applicable PMP in the Measurement Period/number of PMPs If the rationale for rejection of a PMP is a combination of Contractor and County issues, then the applicable Business Hours Delayed on the specific PMP for the purposes of this algorithm will be reduced by 50%, or as mutually agreed-upon by the Parties.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Metric data is created by the Contractor using Service Request Tracking Sheets

11.2 Service Request Schedule Performance

Service Level	Each completed Service Request with an approved PMP. Exclusions: • Firm fixed price Service Requests This SL will be in effect for each in-flight Service Request which had an approved PMP prior to the implementation of this SL. Exceptions to this will be on a case-by-case basis and will be agreed upon prior to the implementation of this SL.		
Service Level ID	49		
Definition	Service Requests completed within last approved schedule excluding any non-approved project revisions as identified via formal change request process.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Schedule	Meet SPI target Monday — Friday 6 a.m. to 6 p.m., excluding the County Holidays	SPI ≥ 0.90	No Earnback provision
Formula	'm' = multiplier for Fee Adjustment calculation. 'm' = 0.05 'n' = factor for Fee Adjustment calculation. 'n' = 165,000 SL Fee Adjustment = m * (n/SPI^2)		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Last approved schedule and SPI		

11.3 Variance to Application Budget

Service Level	Service Request Budget Performance		
Service Level ID	50		
Definition	Measurement of performance to budget and how the Contractor meets its projections excluding any non-approved project revisions as identified via formal change request process.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Budget	Adherence to budget	CPI => 0.90	No Earnback provision
Formula	'm' = Multiplier for fee reduction. 'm'=0.05 Service Level Fee Reduction = m * (Last Approved Budget / CPI)		
Measurement Interval	Each completed Service Request with an approved Project Management Plan (PMP). Exclusions: • Firm Fixed Price Service Requests This Service Level shall be in effect for each in-flight Service Request which had an approved PMP prior to the implementation of this Service Level. Exceptions to this shall be on a case-by-case basis and will be agreed upon prior to the implementation of this Service Level. The types of costs that are to be included in the budget and actual calculations for the Service Level are labor billed through resource units as defined in the Agreement. The fee reduction upper bound is the weighting percentage of the at risk pool.		
Reporting Period	Monthly		
Measurement Tool/Source Data	Last approved budget and CPI		

11.4 Application Availability

Service Level	Measurement of service for general application availability		
Service Level ID	51		
Definition:	The percentage of time that the application is available for normal business operations. Application environments that have performance issues not within control of the Contractor to correct and as demonstrated by the Contractor will be eligible for an exclusion at the County CIO's discretion		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	Available 24/7	99.90% P1, P2 and P3 applications	99.95% P1, P2 and P3 applications
Formula	Total available hours for P1 / total hours in measurement period for P1 AND Total available hours for P2 / total hours in measurement period for P2 AND Total available hours for P3 / total hours in measurement period for P3		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

11.5 Application Availability (Priority 1)

Service Level	Measurement of service for general application availability for Priority 1 (P1) applications		
Service Level ID	51-1		
Definition:	The percentage of time that the application is available for normal business operations. Application environments that have performance issues not within control of the Contractor to correct and as demonstrated by the Contractor will be eligible for an exclusion at the County CIO's discretion		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	Available 24/7	99.90%	99.95%
Formula	Total available hours for P1 / total hours in measurement period for P1		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

11.6 Application Availability (Priority 2)

Service Level	Measurement of service for general application availability for Priority 2 (P2) applications		
Service Level ID	51-2		
Definition:	The percentage of time that the application is available for normal business operations. Application environments that have performance issues not within control of the Contractor to correct and as demonstrated by the Contractor will be eligible for an exclusion at the County CIO's discretion.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	Available 24/7	99.90%	99.95%
Formula	Total available hours for P2 / Total hours in measurement period for P2		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

11.7 Application Availability (Priority 3)

Service Level	Measurement of service for general application availability for Priority 3 (P3) applications		
Service Level ID	51-3		
Definition:	The percentage of time that the application is available for normal business operations. Application environments that have performance issues not within control of the Contractor to correct and as demonstrated by the Contractor will be eligible for an exclusion at the County CIO's discretion.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Availability	Available 24/7	99.90%	99.95%
Formula	Total available hours for P3 / Total hours in measurement period for P3		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Tool supplied by the Contractor automatically records date and time stamps for each activity within a process, including uptime and downtime data		

11.8 Documentation Update Accuracy

Service Level	Measures adherence to update the Applications configuration repository and Application architectural documents
Service Level ID	52

Definition:	Projects that require updates to in-scope artifacts or repositories are refreshed according to the established process
	In scope project items include:
	Architecture Documents (with exclusion of those PAIDs receiving SaaS support):
	• Solution Design Documents required for:
	  o New Implementation of an application
	  o Upgrade of and existing application
	  o Tech Refresh
	• Architecture Diagrams required for:
	  o New Implementation of an application
	  o Upgrade of and existing application
	  o Tech Refresh
	  o TPAR for new/modified firewall rule
	  o Third party IP address change
	
	Specified Apps Manager fields (with exclusion of those PAIDs receiving SaaS support):
	1. Support Bundle – Must be completed.
	2. Application Status – Current Status or Pending Status is set to correct status
	3. Production Release Date –Is set to the date identified for the change to be implemented
	4. NDSR – must be yes if an NDSR is identified during the project and reset to 'No' when the NDSR Period of Performance has expired.
	5. Certificates (If none-"None" in name field)
	  a. Name - cannot be blank
	  b. Type - cannot be blank
	  c. Issuer - cannot be blank
	  d. Expired Date - cannot be blank
	  e. Issue Date - cannot be blank
	  f. Contractor Contact Email - cannot be blank
	6. Servers (X number of servers)
	  a. Server Name - cannot be blank
	  b. Server Environment - cannot be blank
	  c. Server Location - cannot be blank
	  d. Server Purpose - cannot be blank

	7. Software (X items of s/w needed for the application) a. Name – updated/entry created if RFC identifies that SW was installed, removed or updated. b. Version – updated/entry created if RFC identifies that SW was installed, removed or updated. c. Vendor – updated/entry created if RFC identifies that SW was installed, removed or updated. 8. Application Associations/Dependencies a. PAID – updated/entry created if RFC identifies application association. b. App Name/Dependency Type – updated/entry created if RFC identifies application association. c. Portfolio – updated/entry created if RFC identifies application association. 9. Application Interfaces a. Name – updated/entry created if RFC identifies interface. b. Description – updated/entry created if RFC identifies interface. c. Type – updated/entry created if RFC identifies interface. d. Frequency – updated/entry created if RFC identifies interface. 10. MSI a. Name – updated/entry created if RFC identifies new, removed or updated MSI. 11. Active Directory (AD)/Service Account (SVC) a. Name – updated/entry created if RFC identifies new, removed or updated Service Account or AD Account. b. Type – updated/entry created if RFC identifies new, removed or updated Service Account or AD Account. 12. Document Link to current Configuration Instructions a. Doc Type – must be completed b. Name – must be completed c. Link – must be completed and linked documents must be updated as validated by the 'Modified' date in the file properties of the configuration instruction. 13. Document Link to current Installation Instructions a. Doc Type – must be completed b. Name – must be completed c. Link – must be completed and linked documents must be updated as validated by the 'Modified' date in the file properties of the Installation Instructions. 14. Document Link to current Architecture Diagram a. Doc Type – must be completed b. Name – must be completed c. Link – must be completed and linked documents must be updated as validated by the 'Modified' date in the file properties of the Architecture Diagram.

	15. Document link to current Solution Design Document a. Doc Type – must be completed b. Name – must be completed c. Link – must be completed and linked documents must be updated as validated by the 'Modified' date in the file properties of the SDD.		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Document updated	In Scope documents updated per schedule. Schedule will be derived from open actions during CRCB readiness review. Readiness review items determined from the weekly Approved RFC's spreadsheet used by the CRCB.	95%	97.5%

Formula	For documented RFCs: Total in scope documents and Apps Manager fields completed correctly and those that met action due dates as identified during Review /total in scope documents and Apps Manager fields for documented RFCs Each in scope document is counted separately. Each in scope Apps Manager field is counted separately.
Measurement Interval	Monthly
Reporting Period	Monthly
Measurement Tool/Source Data	Document and field compliance are measured and documented during the Change control process. The source data that triggers an event to be in-scope for this SL is the weekly Approved RFC's spreadsheet. The Gate Review Coordinator resource documents compliant items and necessary actions in the Gate Visibility Board and tracks to completion. Schedule is identified as action date on the Visibility board and 95% of those follow up dates are met. Maximum due date is 15 business days from Apps Manager actions identified. For instances where a new or updated SDD or Architecture diagram is required, the new/updated SDD or Architecture diagram would be submitted to EA for approval within 15 business days. SL for each artifact is measured based on the identified completion month of the last action due date for that artifact, not the completion month of the associated RFC.

11.9 Application Response Time

<table>
<tr><td>Service Level</td><td colspan="3">Response Time of the Application for End-User to include all functions of the Application. Application environments that have performance issues not within control of the Contractor to correct and as demonstrated by the Contractor will be eligible for an exclusion at the County CIO’s discretion.</td></tr>
<tr><td>Service Level ID</td><td colspan="3">53</td></tr>
<tr><td>Definition</td><td colspan="3">Effective Response Time for End-Users accessing the Application</td></tr>
<tr><td>Service Measure</td><td>Performance Target</td><td>SL Performance (%)</td><td>SL Earnback</td></tr>
<tr><td>Response Time</td><td>Response Time 24/7 <2 seconds</td><td>Aggregate 98% Per Application</td><td>NA</td></tr>
<tr><td>Formula</td><td colspan="3">Use the Step Reduction Schedule Table to determine the applicable Fee Reduction percentage and subsequently calculate the Fee Reduction amount for a given month. Determine the Fee Reduction percentage based on sum total of Applications that missed the SL Performance and interval in which given month occurs. For example, in January 2022, two Priority 1 Applications missed the SL Performance. Since January 2022 is in the ‘Months 1-9’ interval, a 50% Fee Reduction percentage applies for calculating the Fee Reduction amount.

Step Reduction Schedule Tables for Priority 1, 2, and 3 Applications:
<table>
<tr><th>Priority 1 Applications</th><th>October 2021 – August 2023</th><th>September 2023 and after</th></tr>
<tr><th>Fee Reduction Percentage</th><th>Applications Missing Target</th><th>Applications Missing Target</th></tr>
<tr><td>0%</td><td></td><td></td></tr>
<tr><td>25%</td><td></td><td></td></tr>
<tr><td>50%</td><td>1</td><td>1</td></tr>
<tr><td>100%</td><td>2+</td><td>2+</td></tr>
</table>
<table>
<tr><th>Priority 2 Applications</th><th>October 2021 – August 2023</th><th>September 2023 and after</th></tr>
<tr><th>Fee Reduction Percentage</th><th>Applications Missing Target</th><th>Applications Missing Target</th></tr>
<tr><td>0%</td><td>1-2</td><td>0-1</td></tr>
<tr><td>25%</td><td>3-5</td><td>2-3</td></tr>
<tr><td>50%</td><td>6-8</td><td>4-5</td></tr>
<tr><td>100%</td><td>9+</td><td>6+</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>Priority 3 Applications</th><th>October 2021 – August 2023</th><th>September 2023 and after</th></tr>
<tr><th>Fee Reduction Percentage</th><th>Applications Missing Target</th><th>Applications Missing Target</th></tr>
<tr><td>0%</td><td>1-2</td><td>0-1</td></tr>
<tr><td>25%</td><td>3-5</td><td>2-3</td></tr>
<tr><td>50%</td><td>6-8</td><td>4-5</td></tr>
<tr><td>100%</td><td>9+</td><td>6+</td></tr>
</table>
</td></tr>
<tr><td>Measurement Interval</td><td>Monthly</td></tr>
<tr><td>Reporting Period</td><td>Monthly</td></tr>
<tr><td>Measurement Tool/Source Data</td><td>Measured based on submittals that incorporate measurements from Application Performance Management tool</td></tr>
</table>

11.10 Root Cause Analysis Action Closure

Service Level	Root Cause Analysis Corrective and Preventative Action Completion		
Service Level ID	55		
Definition	Closure of identified corrective and preventative actions from Root Cause Analyses (SL 24)		
Service Measure	**Performance Target**	**SL Performance (%)**	**SL Earnback**
Elapsed Time to produce RCA report	Actions closed within published timeframe (subject to mutual agreement)	99%	99.5%
Formula	Number of instances within Performance Target/total number of instances during Measurement Interval For clarity – actions requiring CoSD approval/support may be excluded subject to mutual agreement.		
Measurement Interval	Monthly		
Reporting Period	Monthly		
Measurement Tool/Source Data	Measured by the Problem management system		

12 TRANSITION SERVICE LEVELS

The County recognizes that transitioning from one primary Contractor to another requires a unique level of cooperation and facilitation between the Legacy Provider and the Contractor. In general, the Contractor will assume responsibility for Service Framework-specific Service Levels upon Cutover of the applicable Service Framework. The Contractor will not be responsible for Service Levels (or portions of Service Levels) relating to Service Frameworks that are not within its control. For Service Levels that span Service Frameworks (e.g., Incident Service Levels), the Contractor shall have responsibility when the fix is within a Service Framework for which the Contractor has already assumed control and responsibility.

13 SPECIAL REQUIREMENTS

In addition to Service Levels, Contractor shall comply with the Special Service Levels specified in Schedule 4.8 Services Levels - Exhibit 4.8-1 Special Service Levels.

14 NETWORK CREDIT TABLE EXAMPLES

SL36b and 36c shall compute SL credits based on the following:

Network Availability: Allow 1 failure for availability target every 100 sites (rounded up)

0% of allocated weight if # of failures is less than or equal to allowable failures

25% of allocated weight if # of failures exceeds allowable failures

50% of allocated weight if # of failures exceeds 2x allowable failures

100% of allocated weight if # of failures exceeds 3x allowable failures

For clarity, if the number of sites is 1 to 100, the allowable failure count is 1; if the number of sites is 101 to 200, the allowable failure count is 2; if the number of sites is 201 to 300, the allowable failure count is 3, etc.

Examples based on 125 T1 sites and 171 Fiber sites (1 allowable failure for T1, 2 allowable failures for Fiber):

Example #1 - One "Fiber" location does not meet its individual availability target; no SL credit is due to the County

Example #2 - Three "Fiber" locations do not meet their individual availability targets; an SL credit of 25% of the allocated weight is due to the County

Example #3 - Three "Fiber" locations do not meet their individual availability targets and three "T1" locations do not meet their individual availability targets; an SL credit of 75% of the allocated weight is due to the County (25% + 50%)

Example #4 - Three "Fiber" locations do not meet their individual availability targets; six "T1" locations do not meet their individual availability targets; an SL credit of 100% of the allocated weight is due to the County (25% + 100%; however the maximum credit due is capped at 100% of the assigned weight)

END OF SCHEDULE

Exhibit 4.8-1 – Special Service Level Requirement

Table of Contents

1. Overview 4
2. Registrar of Voters Special Level (SL) Support 4
2.1. Overview 4
2.1.1. Statewide Elections 4
Election Support Coordination 4
2.1.2. Special Election 4
2.1.3. Small and/or Non Statewide Elections 5
2.2. SL Support Components 5
2.2.1. Immediate Response 5
2.2.2. Escalated Priority 5
2.2.3. Dedicated Onsite Support 5
2.2.4. Freeze on Network Changes 7
2.2.5. Election Support Coordination 7
2.3. Notification 8
3. Treasurer-Tax Collector Special Service Level (SL) Support 8
3.1. Overview 8
3.1.1. Tax Collection Event 8
3.1.2. Tax Sale Event 9
3.2. Special SL Requirements 9
3.2.1. Immediate Response 9
3.2.2. Escalated Priority 9
3.2.3. Dedicated Onsite Support 9
3.2.4. Tax Event Engineering Services 10
3.2.5. Applications Services 10
3.2.6. Other Technical Support 10
3.2.7. Tax Event Support Coordination 10

3.4. Table TTC-2: Tax Sale Event Special SL Support Activities Timeline 12

3.5. Notification 13

4. Assessor/Recorder/County Clerk Acclaim Special Service Level (SL) Support 14

4.1. Overview 14

4.2. Definitions 14

4.3. Special SL Support Services 14

4.4. Notification 16

1. OVERVIEW

The County may require an escalated level of support, referred to as Special Service Level (SL) support, to meet business needs. The Contractor shall, at minimum, perform the Special SL support requirements set forth in this Schedule.

2. REGISTRAR OF VOTERS SPECIAL LEVEL (SL) SUPPORT

2.1. Overview

Contractor shall provide Special SL support for the Registrar of Voters (ROV) as described herein to support Statewide and Special elections.

2.1.1. Statewide Elections

The ROV requires Special SL support during Statewide Elections. The period of Special SL support is typically five (5) months, beginning one hundred and twenty (120) calendar days before Election Day and thirty (30) calendar days after Election Day. The ROV will define the actual period of support and notify Contractor accordingly per Notification procedures outlined in this Schedule.

During the period of Special SL support, the following apply:

- Immediate Response
- Escalated Priority
- Freeze on Network Changes
- Onsite Support

2.1.2. Election Support Coordination Special Election

The ROV requires Special SL support during Special Elections, which may include non-statewide and countywide elections. The period of Special SL support is typically a thirty (30) calendar day period, beginning twenty-nine (29) calendar days before Election Day and the day of the Election. The ROV will define the actual period of support for each election and notify Contractor accordingly per Notification procedures outlined in this Schedule. The ROV also reserves the right to invoke Statewide Election SL for Special Elections.

During the period of Special SL support, the following apply:

- Immediate Response

- Escalated Priority
- Freeze on Network Changes

2.1.3. Small and/or Non Statewide Elections

For small and/or non-statewide Special Elections, the ROV may not engage Special SL support. Additionally, non-statewide Special Elections will not receive the dedicated onsite coverage as shown in Table ROV-1. However, the ROV also reserves the right to invoke Statewide Election SL for Small and/or Non-Statewide Elections.

2.2. SL Support Components

2.2.1. Immediate Response

During the period of Special SL support, all election-related IT and/or telecommunication issues communicated to Contractor shall require immediate response meaning that the appropriate Framework(s) and personnel shall be engaged to restore normal operation without delay.

Immediate response shall also be afforded to ROV Service Requests during the period of Special SL support. Additionally, priority is given to infrastructure and application projects identified as supporting an election.

2.2.2. Escalated Priority

During the period of Special SL support, all election-related IT and/or telecommunication tickets are handled as Priority 1; however, these do not count toward the calculation of the SL achievement.

2.2.3. Dedicated Onsite Support

Contractor personnel shall be physically present at the ROV during the period of Special SL support set forth in Table ROV-1. Contractor personnel not included in Table ROV-1 are considered on-call. The Dedicated Onsite Support requirement may be shortened with the concurrence of ROV and FGG GITM.

The following apply to Dedicated Onsite Support:

- One hour break for meals are permissible during the period of Special SL support.

- Support may be provided in shifts provided the start and end times of each shift is staggered to provide continuity of support.
- Security, Applications, firewall rule and Framework management support are all provided on an on-call/as-required basis throughout the period of Special SL support.
- Dedicated onsite support for cell phone services is provided under a separate Service Request and is not part of Special SL support.

2.2.3.1. Table ROV-1

Resource	Period of Onsite, Dedicated Support	Comments
Election Coordination Manager	1. Twelve (12) calendar days prior to Election Day 8:00 AM – 5:00PM 2. Election Day 6:30AM - close	1. Provides coordination support as required throughout entire Special SL Support period, including onsite attendance at key meetings. 2. Sufficiently qualified personnel may include Desktop Services Manager or a Framework Manager. 3. Coordinate desktop and server patches to not interfere with election operations.
Desktop Technician	1. Twelve (12) calendar days prior to Election Day 8:00 AM – 5:00PM 2. Election Day 6:00AM - 10:00PM	On-site support for Voter's Choice Act (VCA) laptops including break/fix and image configuration.
Telecommunications Management Support	1. Four (4) days prior to Election Day 8:00 AM – 5:00PM (days selected by the ROV) 2. Election Day 6:00AM -10:00PM	On-site support for voice and data services.
Telecommunications Voice System Support	1. Six (6) days prior to the Election Day 8:00AM – 5:00PM (days selected by ROV)	Requires call center/ACD Specialist.

Resource	Period of Onsite, Dedicated Support	Comments
	2. Election Day 6:00AM - 10:00PM	
Network Engineer	1. Seven (7) days prior to Election Day 8:00AM – 5:00PM (days selected by ROV) 2. Election Day 6:00AM - 10:00PM	1. Check Cradlepoint devices for connectivity. 2. Ensure all devices are loaded with an AT&T and Verizon SIM card for redundancy. 3. Fail over SIM cards if primary connection is unstable. 4. Fix Cradlepoint devices at ROV. 5. Network support as needed.

2.2.4. Freeze on Network Changes

The period of Special SL support establishes a 'freeze' on network changes that may impact ROV. However, the 'freeze' may be waived for certain changes and/or the 'freeze period' may be shortened with concurrence of the ROV, FG3 GITM and CTO.

2.2.5. Election Support Coordination

Contractor shall provide an Election Coordination Manager for the management of all Special SL support activities. The Election Coordination Manager is responsible for the coordination of election-related projects, requests and Problem resolution activities. The Election Coordination Manager must be qualified to manage all different Frameworks that may be engaged to support the election. Additionally, the Election Coordination Manager must have the authority to escalate and secure resources as needed for IT and telecommunication issues that arise during the period of Special SL support.

Election Coordination Manager Support activities include, but are not limited to:

- Capacity analysis and Service provisioning for phone systems/hotlines.
- Capacity analysis and provisioning of End User devices (VCA laptop image, VCA laptop).
- Capacity analysis and provisioning for any needed changes or improvements of network equipment (switches, routers, virtual circuits, Cradlepoint devices, cache boxes, etc.).

- Coordination and management of any Third-Parties or Services procured through Contractor to provide election-related Services.
- Coordination of any Services with ROV engaged Third-Parties.
- Coordination of modifications to existing process documentation and Service Desk scripts
- Securing and managing staff assigned to support the election process.
- Coordination of other tasks as requested to support election processes.

2.3. Notification

The ROV or the FG3 Executive Office shall invoke the Special SL support via a Service Request (SR). An authorized SR that the Contractor receives includes the start and end of the period of Special SL support.

For designated Statewide Elections requiring the dedicated onsite support described under Period of Onsite, Dedicated Support in Table ROV-1, the period of Special SL support must be initiated for a minimum period of ninety (90) calendar days prior to the election and continue for a period of thirty (30) calendar days following the Election. Notification

3. TREASURER-TAX COLLECTOR SPECIAL SERVICE LEVEL (SL) SUPPORT

3.1. Overview

Contractor shall provide Special SL support for the San Diego County Treasurer Tax Collector (TTC) as described herein to support Tax Collection and Tax Sale Events.

3.1.1. Tax Collection Event

TTC requires Special SL support during two (2) annual Tax Collection Events. A Tax Collection Event facilitates the payment of annual property tax installments, due April 10th and December 10th. The day of the due date and the days leading up to it generate a heavy load of payments for processing. Special SL support ensures that TTC is able to provide tax collection services efficiently thereby meeting the needs of its customers.

TTC will define the period of Special SL support for each Tax Collection Event and notify Contractor accordingly per Notification procedures outlined in this Schedule. The Contractor shall,

at minimum, provide all requirements outlined in Special SL Requirements and Table TTC-1: Tax Collection Event Special SL Support Activities Timeline during this period.

3.1.2. Tax Sale Event

TTC requires Special SL support for the annual Tax Sale Event, which generally occurs in the spring. The Tax Sale Event facilitates the sale of tax-defaulted property for the sole purpose of recovery of back taxes. The Tax Sale Event is held on a non-county site within San Diego County and may be conducted in conjunction with another County department and/or an online event.

TTC will define the period of Special SL support for each Tax Sale Event and notify Contractor accordingly per Notification procedures outlined in this schedule. The Contractor shall, at minimum, provide all requirements outlined in Special SL Requirements and Table TTC-2: Tax Sale Event Special SL Support Activities Timeline during this period.

3.2. Special SL Requirements

3.2.1. Immediate Response

During the period of Special SL support, all event-related IT and/or telecommunication issues communicated to Contractor shall require immediate response meaning that the appropriate Service Framework(s) and personnel shall be engaged to restore normal operation without delay.

Immediate response shall also be afforded to TTC Service Requests during the Special SL support period. Additionally, priority is given to infrastructure and Application projects identified as supporting the Tax Event.

3.2.2. Escalated Priority

During the period of Special SL support, all tax event related IT and/or telecommunication Tickets are handled as Priority 1; however, these do not count toward calculation of SLs.

3.2.3. Dedicated Onsite Support

Contractor personnel shall be physically present at the TTC during period of Special SL support as set forth in Table TTC-1: Tax Collection Event Special SL Support Activities Timeline and TTC-

2: Tax Sale Event Special SL Support Activities Timeline. Contractor personnel not included in Tables TTC-1 and TTC-2 are considered on-call during the period of Special SL support.

3.2.4. Tax Event Engineering Services

Contractor shall provide Engineering Services resources to support the following:

- Provide support for tax event-related meetings, both scheduled and ad hoc
- Set up training rooms
- Set up Tax Event facilities
- Manage PC and printer hardware setup, delivery and breakdown
- Train County staff
- Provide Tax Event support

3.2.5. Applications Services

Contractor shall provide Applications Services support during the Special SL support period upon TTC request. An authorized Service Request documenting activities and tasks required of Application Services Framework must be received by Contractor for each Tax Event requiring Application Services support.

3.2.6. Other Technical Support

Contractor shall make available a network project manager for meetings set forth in Table TTC-1: Tax Collection Event Special SL Support Activities Timeline and TTC-2: Tax Sale Event Special SL Support Activities Timeline.

Contractor shall make available Network and Desktop Assets required to support Tax Events. An authorized Service Request documenting Assets needed must be received by Contractor for each Tax Event requiring Network and Desktop Assets.

3.2.7. Tax Event Support Coordination

Contractor shall provide a Tax Event Coordination Manager for the management of all Special SL support activities. The Tax Event Coordination Manager is responsible for the coordination of Projects, requests and Problem resolution activities related to the Tax Event. The Tax Coordination Event Manager must be qualified to manage all Frameworks that may be engaged to support the Tax Event. Additionally, the Tax Event Coordination Manager must have the authority to escalate

and secure resource as needed for IT and telecommunication issues that arise during the period of Special SL support.

Tax Event Coordination Manager Support activities include, but are not limited to:

- Development and execution of the Tax Event Project Plan
- Coordination of Tax Event set up and testing
- Oversight of provisioning any needed changes in network equipment
- Management of any Third-Parties or Services procured through Contractor to provide Tax Event related Services
- Coordination of Contractor-provided IT services with TTC engaged Third-Parties
- Securing and managing staff assigned to support Tax Events
- Coordination of other tasks required to provide support for Tax Events
- Coordination with Applications project managers or Applications Technical Leads (ATLs) regarding Service Requests performed in support of Tax Events

3.3. Table TTC-1: Tax Collection Event Special SL Support Activities Timeline

From	Thru	Task	Frequency	Role
LTD - 42	LTD - 42	Participate in Project Kick-Off Meeting with County	Once	Project Manager
LTD - 42	LTD - 42	Participate in Project Kick-Off Meeting with County	Once	Network
LTD - 42	LTD - 42	Develop Scope of Work Document	Once	Project Manager
LTD - 42	LTD - 42	Develop Communications Plan Document	Once	Project Manager
LTD - 42	LTD - 42	Plan Project	Once	Project Manager
LTD - 35	LTD - 35	Develop Project Plan Document	Once	Project Manager
LTD - 13	LTD - 13	Prep and Image 8 Temporary Workstations	Once	Desktop Engineer
LTD - 11	LTD - 11	Deploy Temporary Workstations at CAC	Once	Desktop Technician
LTD - 11	LTD-5	Support Testing of Temporary Workstations at CAC (On-Call)	Once	Desktop Technician
LTD - 11	LTD - 11	Install Temporary Network Connections	Once	Network RU
LTD - 11	LTD - 11	Install Temporary Visa Phone Sets (CAC & Branches)	Once	Network RU
LTD - 4	LTD - 4	Move Equipment from Test Location to Event Location	Once	Desktop Technician

From	Thru	Task	Frequency	Role
LTD - 3	LTD - 1	Provide On-site Desktop Support		Desktop Technician
LTD - 3	LTD - 1	Provide On-call Project Management Support		Project Manager
LTD - 3	LTD -3	Begin Escalation/P1 Response for TTC Tax Collection Outages	All	All
LTD	LTD	Provide On-site Desktop Support		Desktop Technician
LTD	LTD	Provide On-call Project Management Support		Project Manager
LTD + 1	LTD + 1	Remove and Return Temporary Equipment	Once	Desktop Technician
LTD + 1	LTD + 1	End Escalation/P1 Response for TTC Tax Collection Outages	All	All
LTD + 7	LTD + 7	Document Lessons Learned	Once	Project Manager
LTD + 14	LTD + 14	Conduct Project Close-Down	Once	Project Manager
LTD - 42	LTD	Conduct Recurring Planning Meetings with CoSD	6X	Project Manager
LTD - 42	LTD +14	Coordinate Project Activities		Project Manager

LTD = Last Tax Due Date (the last day taxes may be paid by county residents before payment is considered delinquent)

3.4. Table TTC-2: Tax Sale Event Special SL Support Activities Timeline

From	Thru	Task	Frequency	Role
TSD - 56	TSD - 56	Participate in Project Kick-Off Meeting with County	Once	Project Manager
TSD - 56	TSD - 56	Participate in Project Kick-Off Meeting with County	Once	Network
TSD - 56	TSD - 56	Develop Scope of Work Document	Once	Project Manager
TSD - 56	TSD - 56	Develop Communication Plan Document	Once	Project Manager
TSD - 56	TSD - 56	Plan Project	Once	Project Manager
TSD - 49	TSD - 49	Develop Project Plan Document	Once	Project Manager
TSD - 35	TSD - 35	Build/Install Primary Server	Once	Desktop Technician
TSD - 35	TSD - 35	Build/Install Backup Systems	Once	Desktop Technician
TSD - 35	TSD - 35	Build/Install POS Systems	Once	Desktop Technician

From	Thru	Task	Frequency	Role
TSD - 28	TSD - 28	Deploy Temporary Workstations at CAC	Once	Desktop Technician
TSD - 28	TSD	Support Temporary Workstation Testing at CAC	Once	Desktop Technician
TSD - 21	TSD - 14	Training Session Support (1 FTE @ 4 Hour Session)	Once	Desktop Technician
TSD-3	TSD-3	Begin Escalation/P1 Response for TTC Tax Sale Outages		All
TSD	TSD	Move Equipment to Tax Sale Site & Test	Once	Desktop Technician
TSD	TSD	Install Switches for Stand-Alone Network	Once	Desktop Technician
TSD	TSD	Onsite Desktop Support (2 FTE @ 4 Hours each)	Once	Desktop Technician
TSD	TSD	Remove and Return Equipment	Once	Desktop Technician
TSD+1	TSD+1	End Escalation/P1 Response for TTC Tax Sale Outages		All
TSD + 1	TSD + 3	Post-Sale User Support / Verify Successful Migration of POS DB to Production Server	Once	Project Manager
TSD + 7	TSD + 7	Update Tax Sale Support Documentation - Infrastructure	Once	Project Manager
As Sched	As Sched	Participate in CoSD Planning Sessions	4X	Project Manager
Dec	Mar	Data Network On-Call Support	As Required	Network
Dec	Mar	Provide P1 response on TTC Tax Sale DB/TRDS/Maps & Images	All	All
Dec	Mar	Provide P1 response on PCs/Servers/Citrix For TTC Tax Sale Users	All	All

TSD = Tax Sale Date (the date of the Tax Sale event)

3.5. Notification

The TTC or FG3 Executive Office shall invoke the Special SL support via a Service Request. An authorized Service Request must be received by Contractor sixty (60) calendar days prior to the date of the Tax Event.

Request for additional days of Special SL support ("Daily Coverage") requires an authorized Service Request to be received by Contractor ten (10) calendar days prior to beginning date of additional coverage.

Daily Coverage Support may be terminated early per TTC request. An authorized Service Request must be received by Contractor three (3) calendar days prior to new end date of Daily Coverage.

4. ASSESSOR/RECORDER/COUNTY CLERK ACCLAIM SPECIAL SERVICE LEVEL (SL) SUPPORT

4.1. Overview

Standard Contractor support coverage for Assessor / Recorder / County Clerk (ARCC) e-Recording comprises of Contractor's e-Recording Coordination Manager being available via business phone, cell phone, or page during normal business hours, and via cell phone or page, in an on-call status, during non-business hours. ARCC is also provided an updated roster of Contractor Desktop Technicians on-call for after hours and weekend issues.

Contractor shall provide Special SL support for ARCC e-Recording as described herein to support the extremely high volume of e-Recording at designated periods throughout the year.

4.2. Definitions

4.2.1. ARCC Month End Event - An extremely high volume of e-Recording is expected the last two business days of each month. During this period, ARCC requires special support of their information technology infrastructure and applications at all ARCC sites.

4.2.2. ARCC Holiday Event - An extremely high volume of e-Recording the business day before and the business day after each official County holiday. During this period, ARCC requires special support of their information technology infrastructure and applications at all ARCC sites.

4.2.3. 'At the ready'- Refers to a heightened state of preparedness. An individual who is 'at the ready' will be in a constant state of preparedness to immediately respond to ARCC calls, be able to immediately access the County network and applications, and take necessary action(s) required to resolve technical issues.

4.3. Special SL Support Services

Special SL Support Services are defined as follows:

4.3.1. Immediate Response - During the period of Special SL support, a problem or outage called in to the Help Desk or communicated to on-site Contractor personnel will result in an immediate

response and effort to resolve the problem. This response is delivered by the appropriate Contractor framework(s) and the personnel necessary to restore operation without delay.

4.3.2. Escalated Priority - During the period of Special SL support, each Special SL-related ticket is handled as a Severity 1 (S1); however, these tickets do not count S1 for SL calculation purposes.

4.3.3. e-Recording Support Coordination - Contractor shall provide an e-Recording Coordination Manager to coordinate all Special SL support services. The e-Recording Coordination Manager is responsible for the coordination of all e-Recording requests and problem resolution activities therefore the designated resource must be qualified to manage all the different frameworks engaged to support e-Recording and must have the authority to escalate tickets and secure necessary resources to resolve any issues.

4.3.4. Applications Support - During the period of Special SL support, the e-Recording Coordination Manager will be 'at the ready' during normal ARCC business hours (08:00 to 17:00 PST) and before-hours (07:00 to 08:00 PST) and after-hours (17:00 to 20:00 PST). The Contractor e-Recording Coordination Manager will own the incident until it is resolved and will work in concert with the Incident Manager to drive the issue to resolution. As the owner of the incident, the Contractor e-Recording Coordination Manager will work with any ARCC 3rd party vendor and any Contractor resources necessary and will take ownership of the incident resolution as the primary vendor for the ARCC.

4.3.5. Incident Management Support - During the period of Special SL support, an Incident Manager will be 'at the ready' during normal ARCC business hours (08:00 to 17:00 PST) and before-hours (07:00 to 08:00 PST) and after-hours (17:00 to 20:00 PST). This elevated support is already funded via the existing infrastructure resource units. The Incident Manager will be immediately available via business or cell phone and will coordinate with the Contractor e-Recording Coordination Manager to:

i. Immediately assess the situation.
ii. Identify and engage the resources necessary to resolve the incident.
iii. Open up a technical bridge, if needed.
iv. Provide regular status to ARCC, CTO, and Contractor from incident report through incident resolution.
v. Ensure that when a multi-user issue is reported, the incident is automatically paged out and Incident Manager is automatically engaged by the Contractor Help Desk.

4.3.6. CAC On-site Support - During the period of Special SL support, an on-site Desktop Technician will be physically at the CAC and 'at the ready' during normal business hours (08:00 to 17:00 PST) and before-hours (07:00 to 08:00 PST) and after-hours (17:00 TO 20:00 PST) while ARCC is operational. The on-site Desktop Technician(s) will provide immediate analysis and resolution of operational related issues. Regular business hours support is already funded via the existing infrastructure resource units. Elevated, after hours, 'at the ready' support will be funded via this Special Level.

4.3.7. Database Administrator (DBA) Support - During the period of Special SL support, a DBA resource will be 'at the ready' during normal ARCC business hours (08:00 to 17:00 PST) and before-hours (07:00 to 08:00 PST) and after-hours (17:00 to 20:00 PST) while ARCC is operational. The DBA will constantly monitor the application database during this time. Regular business hours support is already provided and is funded on a time & materials basis, as needed. Elevated, after hours, 'at the ready' support will be funded via this Special Level.

4.3.8. Additional Support - Along with the elevated, 'at the ready' personnel identified above, Contractor's leveraged resources (System Administrators, Server Administrators, Network Personnel, Security Personnel, etc.) already provide 7x24 coverage and will be on-call to provide elevated support for this Special SL. This elevated support is already funded via the existing infrastructure resource units.

4.3.9. Reporting - Contractor will provide the ARCC with AM, Mid-Day, and PM Systems checks of the (1) database, (2) server, and (3) network.

4.4. Notification

The ARCC or the Finance and General Government Group (FG3) Executive Office initiates Special SL Support Services for ARCC Holiday Event or ARCC Special Support Daily Coverage by submitting an IMAR to Contractor. For Fixed Price Support of ARCC Holiday Event, an IMAR must be received by Contractor at least 30 calendar days prior to the date of the Event, with start and end dates specified. For ARCC Special Support Daily Coverage, an IMAR must be received by Contractor at least ten days prior to start date of the Special SL Support Daily Coverage period, with both the beginning and ending dates specified. In the event that ARCC wishes to terminate Special SL Support Daily Coverage earlier than requested, an IMAR must be received by Contractor at least three days prior to the new end date, with new end date specified.

END OF SCHEDULE

Schedule 5 – Invoices and Reports

Contents

1. Overview 3

2. Objectives 3

3. Deliverables/Reports by Framework 4

1. OVERVIEW

Contractor shall provide usage/inventory data that the County can use to chargeback Contractor's fees to County projects or Departments. This data consists of the quantity of usage or inventory data and an associated County project number or Department, if available and applicable. The data also include a Service identifier linked to a specific billing element, as well as a date of Service, if applicable. Usage data reports must be totaled and summarized by project number and/or Department, as required by the County. Detail and summary information reported monthly in a standard electronic file format provided by the County not later than the 10th of each month, for Services performed in the preceding month.

2. OBJECTIVES

2.1. The Contractor shall provide reports and information to the County to demonstrate the Contractor's compliance with the Service Levels in addition to the reports specified in this Section. Contractor is required to retain data to generate reports for historical purposes during the Term.

2.2. The County will define the requirements for any project numbering system needed to track such elements as mainframe usage or applications maintenance and development hours. The County will also provide and update the Department information that Contractor shall maintain in the inventory databases.

2.3. The County will provide and update the Business Unit (Department) and POETA (Project, Org, Expenditure, Task, and Award) information that Contractor shall maintain in the inventory databases. In addition, Contractor shall create and utilize summary usage report formats, subject to the County's approval, to enable the County to chargeback Contractor's fees.

2.4. During Transition, Contractor shall work with designated personnel from the County to develop specific policies and procedures regarding establishing and using Department/project numbers and establishing/updating Department information for the inventory databases. In addition, with the County's approval, Contractor shall develop summary usage report formats to enable the County to chargeback Contractor's fees.

2.5. Inventory data is a snapshot of the information on the last day of Contractor's accounting month. Usage data reports shall be totaled and summarized by Business Unit (Department) and Business Group, as required by the County. Detail and summary information shall be reported monthly in a standard electronic file format not later than the 10th of each month, for Services performed in the preceding month.

2.6. All reports shall be posted in the online Service Portal that is available to authorized County End-Users.

2.7. The contents of the SnP Manual for all Frameworks shall be referenced in the monthly Schedule 5 report, "Schedule 5 Invoices and Reports List".

2.8. Content management (add/remove/change) of the Schedule 5 Reports will be done with a Service Request.

3. DELIVERABLES/REPORTS BY FRAMEWORK

The Schedule 5 Reports List maintains the deliverables/reports that Contractor is required to provide to the County on a regularly scheduled basis under the Agreement is not intended to be an exhaustive list of each and every report that Contractor is required to provide to the County as specifically required by the Agreement. Contractor shall also provide to the County such additional reports as appropriate from time to time or as the County requests pursuant to Services provided in this Agreement.

END OF SCHEDULE

Exhibit 5.1 – Telecom Fees

Table of Contents

1. Telecom Transport Services 3
2. Charges for Telecom Transport Services 3
3. Quality, Performance and Remedies 3
4. Contractor Not Responsible for Unauthorized Use 3
5. Telecom Usage 4
6. Taxes 4

1. TELECOM TRANSPORT SERVICES

AT&T Corp. and its affiliates (the "Telecom Vendor") are approved subcontractors and are the actual providers of the Telecom Transport Services and that County will receive such Telecom Transport Services from the Telecom Vendor. As used herein, "Telecom Transport Services" means: High Capacity Service, Primary Rate Service, DS3 Service, PBX Trunk Service, Super Trunk Service, SONET Ring and Access Service, GigaMan® Service, Optical Carrier Network Point-to-Point Service, Message Telecommunications Service, Centrex Service, OPT-E-Man® Service, Long Distance Voice Services, SBC PremierSERVSM Frame Relay Service, SBC PremierSERVSM Asynchronous Transfer Mode, SBC PremierSERVSM Dedicated Internet Access, Series and 200 Voice Mail. The Telecom Transport Services are private services and are not common carrier services.

2. CHARGES FOR TELECOM TRANSPORT SERVICES

The service parameters, if any, for the Telecom Transport Services will be those set forth in the applicable tariff, regulations, or service guide of the Telecom Vendor providing the Telecom Transport Services. Peraton Enterprise Solutions LLC (Contractor) shall assist County in the reporting of any problems with the Telecom Transport Services.

3. QUALITY, PERFORMANCE AND REMEDIES

Contractor shall furnish the County Technology Office with a single invoice, inclusive of all charges related to the Telecom Transport Services. Each single invoice shall include an itemized accounting of Resource Units incurred during the immediately preceding month. Below the total charges identified on the single invoice, Contractor shall instruct County what portion of the total charges must be remitted directly to the Telecom Vendor related to the Telecom Transport Services, and the net resulting amount being remitted directly to Contractor. County shall pay this amount to the Telecom Vendor within forty-five (45) days of County's receipt of the single invoice for all Services provided under the Agreement.

4. CONTRACTOR NOT RESPONSIBLE FOR UNAUTHORIZED USE

Contractor will not be responsible for any unauthorized County use of the Telecom Transport Services.

5. TELECOM USAGE

County will maintain policies relative to and provide assistance for: (i) preventing the abuse or fraudulent use of the Telecom Transport Services, (ii) preventing any information, data or message from being transmitted over the network by County which would constitute libel, slander, infringement of copyright, invasion of privacy, violation of trans-border data flow regulations, access or alteration of private or personally identifiable records or data, (iii) any database maintenance functions that may be required to implement E911 service at any County location, or (iv) any compliance that may be required with the Communications Assistance for Law Enforcement Act and related regulations.

6. TAXES

As part of the invoice instructions to be provided to the County by Contractor pursuant to Paragraph 2 above, all fees payable by County to Contractor and the Telecom Vendor (as contained in the single invoice referred to in Paragraph 2 above) shall be inclusive of all taxes, including any applicable telecommunications surcharges or fees, or any related telecommunications taxes imposed, levied, or assessed by government authorities or otherwise charged by the Telecom Vendor on the Telecom Transport Services. Such surcharges, fees or taxes will be included in the amount to be remitted directly to the Telecom Vendor. Contractor acknowledges that County shall have no obligation to pay or be liable for any such surcharges, fees or taxes that may be imposed, levied or assessed "outside of" or in addition to the amounts directly remitted to the Telecom Vendor, as described in Paragraph 2 above.

END OF EXHIBIT

Schedule 7.2 – End-User Satisfaction Surveys

Table of Contents

1. Overview 3

2. Survey Objectives....3

3. Survey Process 3

1. OVERVIEW

For each Service Framework, Contractor shall conduct periodic customer satisfaction surveys to discern End-User perception with respect to Service delivery. Contractor shall ensure that survey results are monitored and reviewed and that necessary corrective actions are taken to improve performance. County shall be informed regularly of survey results per agreed upon format and have input on corrective actions and performance improvement activities.

2. SURVEY OBJECTIVES

2.1. Monitor End-User satisfaction with respect to Service delivery.

2.2. Identify and promptly address less than satisfactory survey results.

2.2. Maintain consistently high End-User satisfaction with respect to Service delivery.

3. SURVEY PROCESS

3.1 Design Survey

Contractor shall design a user-friendly, web-based survey that can be completed within five (5) minutes by an End-User. Contractor shall obtain County approval prior to distribution of a new or modified survey.

3.1 Selection of Survey Population

Contractor shall distribute one thousand (1000) surveys each month across the County. Contractor shall randomly select survey population from Break-Fix (BF) and Service Request (SR) requestors based on BF and SR tickets in active or completed status within the preceding thirty (30) day period. An End-User shall receive no more than two (2) surveys per calendar year.

3.3 Survey Distribution

Contractor shall send notice of survey to survey population via email. The email shall include survey instructions, information about the Break-Fix (BF) and Service Request (SR) for which information is being sought, and a direct link to the web-based survey.

Contactor shall accommodate Business Groups that have in place a centralized SR and BF system by allowing survey to be forwarded to and completed by someone other than the requester.

3.4 Response Monitoring

Contractor shall monitor survey response rate to ensure a one hundred (100) percent completion rate. As needed, Contractor may send a follow up email to End-User requesting completion of survey.

3.5 Survey Results

Contractor shall monitor and maintain survey results. For less than satisfactory results or feedback, the associated BF or SR ticket will be reviewed to establish appropriate corrective actions. Contractor shall report survey results and any associated corrective actions to County per agreed upon format. Contractor shall meet with County on a weekly basis to discuss results and corrective actions.

END OF SCHEDULE

Schedule 7.3.1 – Standards and Procedures

Table of Contents

1. Overview 3

2. High Level Requirements 3

3. Standards and Procedures Manual Topic List 3

1 OVERVIEW

The Standards and Procedures (SnP) Manual lists specific steps to be followed by role who will be held accountable for certain activities. A policy will be formed when there is a need to establish formal policies that the teams must abide by. A policy will often reference a Standards and Procedures Manual for specific steps. In addition to standard procedures, the SnP Manual will also contain all documented standards (e.g. Hardware, Software, bricks and patterns, etc.).

2 HIGH LEVEL REQUIREMENTS

2.1 The SnP Manual shall be posted in the Service Portal.

2.2 The SnP Manual shall be accessible to authorized End-Users to the appropriate Service Framework section(s).

2.3 The SnP Manual shall be assigned a designated document manager responsible for the organization of documents, review periods, posting of completed sections, Service Framework section numbering assignment, etc.

2.4 The SnP Manual shall provide a clear formal procedure to create, update, and maintain the SnP Manual integrity and updated information.

2.5 The contents of the SnP Manual for all Frameworks shall be referenced in the monthly Schedule 5 report, Schedule 7.3.1 List.

2.6 Content management (add/remove/change) of the SnP Manual will be via a Service Request.

3 STANDARDS AND PROCEDURES MANUAL TOPIC LIST

3.1 The SnP Manual topic list will be maintained in the Schedule 5 report**,** "Schedule 7.3.1 Standards and Procedures List".

END OF SCHEDULE

Schedule 7.6 — Shared Resources

Table of Contents

1. Overview 3
2. Cross-Functional Equipment, Software, Tools and Systems....3
3. Service Desk Equipment, Software, Tools and Systems....5
4. End-User Equipment, Software, Tools and Systems....5
5. Network Equipment, Software, Tools and Systems....6
6. Data Center Equipment, Software, Tools and Systems....8
7. Applications Maintenance and Operations Equipment, Software, Tools and Systems....9
8. Applications Development Equipment, Software, Tools and Systems....9

1. OVERVIEW

Contractor shall provide a listing of Shared Resources by Component within each Service Framework in Schedule 7.6 – Shared Resources. For each Shared Resource, the following information shall be included: resource / tool name, type (Software or Machine), manufacturer, version, purpose or use, and any other information of relevance the Contractor deems necessary.

For software or infrastructure that runs in the data center, or as a service, the hardware that runs this software is also a shared resource.

2. CROSS-FUNCTIONAL EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

Resource / Tool Name	Information
Enterprise System List (ESL)	**Type:** Software **Manufacturer:** HPES **Version:** 16.1.1 **Purpose/Use:** ESL (Enterprise System List) is a Delivery focused Configuration Management System for managing System/Application Configuration Items, Services/Contracts and Customer/Account information. **Other Information:**
Asset Manager	**Type:** Software **Manufacturer:** HPE **Version:** 3.7P1 **Purpose/Use:** Tracks end-user and network assets **Other Information:**
Discovery and Dependency Mapping Inventory (DDMI)	**Type:** Software **Manufacturer:** HPE **Version:** 9.32 P1 **Purpose/Use:** discovers and reports assets found on the network; integrates with Asset Manager. **Other Information:**
Service Manager	**Type:** Software **Manufacturer:** HPE **Version:** 4.0.5p31 **Purpose/Use:** Used by the Service Desk and all support staff for ticketing of Incidents, Problems and Changes. **Other Information:**
End User Access (EUA)	**Type:** Software **Manufacturer:** HPES **Version:** 2.1.6 **Purpose/Use:** Service Portal **Other Information:** While the core software and interfaces are standardized and centrally controlled to interact with the rest of the cross

Resource / Tool Name	Information
	functional tools, the Service Portal is separately instantiated and customized for each client for whom it is deployed.
Aries/Aldea	**Type:** Software **Manufacturer:** HPES **Version:** 3.5.6 / 8.9.3 **Purpose/Use:** Tool used by HPES internally to request resources (e.g., staffing assignments, workload placement) from the broader HPE community **Other Information:**
RevGen	**Type:** Software **Manufacturer:** SAP Ariba **Version:** 9r1 **Purpose/Use:** Procurement of products and services **Other Information:**
Enabling Delivery and Global Excellence (EDGE)	**Type:** Knowledge Repository **Manufacturer:** HPES **Version:** 4.3 **Purpose/Use:** EDGE is a holistic environment that includes all the information needed to enable Enterprise Solutions (ES) to deliver and excel in the global marketplace. EDGE supports all individuals in each of the ES business units by providing process artifacts that can be leveraged and used as part of their day-to-day work. **Other Information:**
Enterprise Maps	**Type:** Software **Manufacturer:** HPE **Version:** 3.0 **Purpose/Use:** HPE Enterprise Maps software plans and drives IT transformation roadmaps by mapping the overall IT landscape with business outcomes. **Other Information:** Enterprise Maps is certified as ArchiMate 2 Tool and incorporates principles from TOGAF Enterprise Architecture Framework
Enterprise Architect	**Type:** Software **Manufacturer:** Sparx Systems **Version:** 9.3 **Purpose/Use:** Enterprise Architect provides full life cycle modeling for: Business and IT systems Software and Systems Engineering Real-time and embedded development **Other Information:**
ProVision	**Type:** Software **Manufacturer:** OpenText **Version:** 9.0.2 **Purpose/Use:** ProVision is HPES's standard modeling tool, to be used for Business Process, Enterprise Architecture and IT solution modeling. It enables business & IT teams to visually create models, describing business process, process interactions and detailed workflow **Other Information:**
Disaster Recovery Subscription Services, consisting of all	**Type:** Disaster Recovery Subscription Services **Manufacturer:** various

Resource / Tool Name	Information
leveraged hardware and software used to provide: Server services Storage services Network services Security services Backup services	**Version:** N/A **Purpose/Use:** Leveraged hardware and software **Other Information:** Note that the Centera and the dedicated firewalls located in the DR site are not considered to be part of this list, since they are dedicated to the County.
ArcSight Security Information and Event Management (SIEM)	**Type:** Software/appliance **Manufacturer:** HPE **Version:** 6.9.1 **Purpose/Use:** Event logging and monitoring **Other Information:**
Global Delivery Capacity & Performance Management (GDCPM)	**Type:** Software **Manufacturer:** HPES (based on SAS and other underlying tools) **Version:** 2.0 **Purpose/Use:** Collects, aggregates and analyzes capacity and performance data from various disparate sources for reporting and analysis **Other Information:**

3. SERVICE DESK EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

Software used in providing Service Desk services is listed in the Cross-Functional section, since this software is also used by other frameworks.

IVR and ACD hardware and software, and other tools/facilities used by the Service Desk are internal to Contractor, and are not listed individually

4. END-USER EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

Resource / Tool Name	Information
System Center Configuration Manager (SCCM)	**Type:** Software **Manufacturer:** Microsoft **Version:** 2012 **Purpose/Use:** Discovery and software distribution to end-user devices **Other Information:**

5. NETWORK EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

Resource / Tool Name	Information
Leveraged Internet Service (LIS) firewalls in the Tulsa and Colorado Springs data centers	**Type:** Hardware **Manufacturer:** Checkpoint **Version:** D2 **Purpose/Use:** Internet access/security **Other Information:** In the future these are slated to be replaced by Fortinet firewalls
AT&T Commonly Shared Network	**Type:** Equipment, tools, software, systems and other materials **Manufacturer:** Various **Version:** N/A **Purpose/Use:** For clarity, the AT&T Commonly Shared Network means (i) the public or shared networks of AT&T, its Affiliates and their subcontractors, and the equipment, tools, technologies, systems, software, and other materials that are components thereof; (ii) equipment, tools, technologies, systems, software and other materials used by AT&T, its Affiliates and their subcontractors in shared network management and back office environments including , without limitation, TIRKs, iGEMS, BusinessDirect, Billing Edge, the AT&T Global Network Client and AT&T Connect and any other items listed above in this Exhibit; and (iii) all modifications, upgrades, derivative works, enhancements, improvements and extensions of any of the foregoing.
SIMS (Security Information Management System)	**Type:** Software **Manufacturer:** AT&T **Version:** n/a **Purpose/Use:** Security event correlation **Other Information:**
SDNOM (Software Defined Network Order Management)	**Type:** Software **Manufacturer:** AT&T **Version:** 1.0 Release 1604 **Purpose/Use:** Circuit Ordering **Other Information:**
Nectar Unified Communication Management Platform	**Type:** Software **Manufacturer:** Nectar **Version:** 5.5.2.1 **Purpose/Use:** Voice Network Performance Management **Other Information:**
MDM-Airwatch SaaS Console (Mobile Device Management)	**Type:** Software **Manufacturer:** AT&T **Version:** 8.2 **Purpose/Use:** Mobile device management **Other Information:**
SORD (Service Order Retrieval and Distribution)	**Type:** Software **Manufacturer:** AT&T **Version:** 8.1.10 **Purpose/Use:** Service order entry **Other Information:**
Telegence	**Type:** Software

Resource / Tool Name	Information
	Manufacturer: AT&T **Version:** 1602.3 **Purpose/Use:** Billing **Other Information:**
BOSS (Billing and Ordering Support System)	**Type:** Software **Manufacturer:** AT&T **Version:** 8.1.01 **Purpose/Use:** Product billing, tracking and reporting **Other Information:**
DPSS (Data Products and Services System)	**Type:** Software **Manufacturer:** AT&T **Version:** N/A **Purpose/Use:** Data product and services tracking **Other Information:**
BusinessDirect/eBill	**Type:** Software **Manufacturer:** AT&T **Version:** N/A **Purpose/Use:** Account management **Other Information:**
Exchange Plus	**Type:** Software **Manufacturer:** AT&T **Version:** 13.1 **Purpose/Use:** Carrier resource tracking **Other Information:**
ICES (Integrated Customer Enterprise System) ServiceCenter/AssetCenter	**Type:** Software **Manufacturer:** AT&T **Version:** 5.1.2 **Purpose/Use:** Asset Inventory **Other Information:**
SAINT	**Type:** Software **Manufacturer:** AT&T **Version:** 7.20.13 **Purpose/Use:** Security scanning and testing **Other Information:**
Nmap	**Type:** Software **Manufacturer:** Nmap **Version:** v7.0 **Purpose/Use:** Network scanning and mapping **Other Information:**
WFA (Work Force Administration)	**Type:** Software **Manufacturer:** Telcordia **Version:** n/a **Purpose/Use:** Trouble ticketing and work flow **Other Information:**
TIRKS (Trunks Integrated Record Keeping System)	**Type:** Software **Manufacturer:** Telcordia **Version:** n/a **Purpose/Use:** Circuit design **Other Information:**

Resource / Tool Name	Information
AOTS-TM (AT&T One Ticketing System – Trouble Management)	**Type:** Software **Manufacturer:** AT&T/Remedy **Version:** n/a **Purpose/Use:** trouble ticketing **Other Information:**
NMA (Network Monitoring and Analysis)	**Type:** Software **Manufacturer:** Telcordia **Version:** n/a **Purpose/Use:** Network monitoring **Other Information:**
Avaya Site Administration	**Type:** Software **Manufacturer:** Avaya **Version:** 6.0 **Purpose/Use:** Voice system administration **Other Information:**

6. DATA CENTER EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

Resource / Tool Name	Information
Server Automation	**Type:** Software **Manufacturer:** HPE Software **Version:** 10.11 **Purpose/Use:** Distributing operating system and layered product patches and upgrades **Other Information:** The core mesh is a shared resource; distribution satellite servers within the County's network zones are dedicated to the County
Operations Manager	**Type:** Software **Manufacturer:** HPE Software **Version:** 9.2 **Purpose/Use:** Monitoring and alerting for various data center components, such as servers, domain controllers, databases, etc.
Microsoft Office 365 Government Community Cloud	**Type:** Software as a Service **Manufacturer:** Microsoft **Version:** 2016 **Purpose/Use:** E-Mail (Exchange Online), Collaboration (SharePoint Online, Skype for Business), Cloud File Management (OneDrive for Business)
E2E Complete	**Type:** Software **Manufacturer:** BinaryTree **Version:** 4.0 **Purpose/Use:** Automation tool for migration of mail services from Exchange to the Microsoft Office 365 Cloud
Helion Virtual Private Cloud for US Public Sector	**Type:** Infrastructure as a Service **Manufacturer:** HPE **Version:** 7.6

Resource / Tool Name	Information
	Purpose/Use: Virtual Private Cloud (VPC) for Windows and Linux environments. VPC is a Government Community Cloud currently used to run the County's Beach and Water Quality website.
Watchdog	**Type:** Software **Manufacturer:** HPES **Version:** N/A **Purpose/Use:** Internally developed utility that monitors/removes privileged access implemented via non-approved methods

7. APPLICATIONS MAINTENANCE AND OPERATIONS EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

All tools identified for applications development may also be used in the applications Maintenance and Operations (M&O) environment.

8. APPLICATIONS DEVELOPMENT EQUIPMENT, SOFTWARE, TOOLS AND SYSTEMS

Resource / Tool Name	Information
StarTeam	**Type:** Software **Manufacturer:** Microfocus/Borland **Version:** N/A **Purpose/Use:** Software Change and Configuration Management **Other Information:** This tool may also be used in Business Analysis and Applications M&O
Together	**Type:** Software **Manufacturer:** Microfocus/Borland **Version:** N/A **Purpose/Use:** Together enables software to be designed using industry-standard UML notation and conventions. With a large number of built-in utilities to manage the software design process, validate designs and generate code, Together helps maximize the efficiency and accuracy of the software development process **Other Information:** This tool may also be used in Business Analysis and Applications M&O
Agile Manager	**Type:** Software **Manufacturer:** HPE **Version:** N/A **Purpose/Use:** Agile project management is a SaaS (software-as-a-service) solution that helps teams to organize, plan, and execute Agile projects. **Other Information:** This tool may also be used in Business Analysis and Applications M&O
Team Foundation Server	**Type:** Software **Manufacturer:** Microsoft **Version:** N/A

Resource / Tool Name	Information
	Purpose/Use: Microsoft Team Foundation Server (TFS) is a set of tools and technologies that enable a team to collaborate and coordinate the development and build efforts for a .NET software product or completing a .NET software project. **Other Information:** This tool may also be used in Business Analysis and Applications M&O

END OF SCHEDULE

Schedule 8.1 – License for Use of County Facilities and Property

LICENSE FOR USE OF COUNTY FACILITIES AND PROPERTY

This license agreement ("License") is entered into on _____ between the County of San Diego, a political subdivision of the State of California ("County"), and Peraton Enterprise Solutions LLC ("Licensee").

RECITALS

A. Licensee wishes to the use County-owned property ("Property") defined in Section 1 Premises for _____.

B. County is willing to permit Licensee to use the Property subject to the terms and conditions contained in this License.

C. Unless otherwise set forth herein, all terms in this License shall be as defined in the Information Technology and Telecommunications Service Agreement between the County of San Diego and _____ dated _____ ___, 2016.

LICENSE

1. Premises. Licensee may use _____San Diego, California. The _____ are collectively referred to in this License as the "Premises", and are further described in Exhibit "A" DESCRIPTION OF PREMISES of this License.

2. Term. The term of this License commences on the Effective Date of the Information Technology and Telecommunications Service Agreement between the County of San Diego and _____ dated _____ ___, 2016, and expires the end of the Initial Term and any Renewal Term(s).

3. Use. Licensee may use the Premises for the sole purpose of providing the Services. Licensee is not authorized to use the Premises on any other days or at any other times other than the times stated in Section 2 Term or use any other part of the Premises not described in Exhibit "A". If the County's Director, Department of General Services ("Director") determines that Licensee's use of the Premises on these days and/or at these times

would in any way conflict or be inconsistent with the conduct of County business, the Director may unilaterally change the days and/or times Licensee may use the Premises or may terminate this License immediately without incurring any liability to Licensee.

4. Access. Licensee shall not impede the flow of vehicular traffic on, or restrict public access to or from, the Property. Licensee shall not interfere with County operations at the Property or Premises. When on the Property and Premises, Licensee and Licensee's guests and invitees shall drive only on established roadways and driveways.

5. License. This License is not a lease, does not create or convey an easement and does not convey any interest or estate in real property to Licensee. County may terminate this License at any time. County may enter the Premises covered by this License at any time.

6. Insurance. Licensee shall comply with the Insurance Requirements set forth in the Information Technology and Telecommunications Service Agreement between the County of San Diego and _____ dated _____ ___, 2016.

7. License Fee. In accordance with the County Board of Supervisors Policy B-29, Fees, Grants, Revenue Contracts - Department Responsibility for Cost Recovery, the County is receiving full compensation for the license through the Agreement and Contractor's provision of Services therein.

8. Defense and Indemnity. To the fullest extent permitted by law, County shall not be liable for, and Licensee shall defend and indemnify County and its elected officials, officers, agents, employees and volunteers (collectively, "County Parties"), against any and all claims, deductibles, self-insured retentions, demands, liability, judgments, awards, fines, mechanics' liens or other liens, labor disputes, losses, damages, expenses, charges or costs of any kind or character, including attorneys' fees and court costs (collectively, "Claims"), that arise out of or are in any way connected to this License or Licensee's use of the Premises arising either directly or indirectly from any act, error, omission or negligence of Licensee or its officers, employees, agents, contractors, licensees, servants, guests or invitees including, without limitation, Claims caused by the sole passive negligent act or the concurrent negligent act, error or omission, whether active or passive, of County Parties. Licensee shall have no obligation, however, to defend or indemnify County Parties from a Claim if it is determined by a court of competent jurisdiction that the Claim was caused by the sole active negligence or willful misconduct of County Parties.

9. Maintenance, Cleanup and Repair. Licensee shall conduct its operations in an orderly manner and shall leave the Premises in as clean and good a condition as when Licensee entered the Premises pursuant to this License. If Licensee damages any County property or facilities or incurs excessive cleanup of the Premises, Licensee shall promptly inform the Director and shall promptly reimburse the County for the full costs that County incurs to repair the damage or replace the item.

10. Storage. Licensee shall not store or leave any personal property or equipment on or in the Premises without obtaining the prior written consent of the Director of General Services.

11. License on Site. Licensee shall have a copy of this License available at all times when Licensee is using the Premises. Licensee shall show a copy of this License to County staff upon request.

12. Compliance with Stormwater Laws. Licensee's use of the Premises is subject to all present or future federal, state and local laws, statutes, regulations, ordinances, policies, guidelines and orders ("Stormwater Laws") regarding the discharge of pollutants into the stormwater conveyance system. Licensee's compliance with Stormwater Laws may include requirements for Licensee to develop, install, implement and maintain pollution prevention measures, source control measures and Best Management Practices ("BMPs"). BMPs can include operational practices, water or pollutant management practices, physical site features, or devices to remove pollutants from stormwater, to affect the flow of stormwater or to infiltrate stormwater to the ground. BMPs applicable to Licensee's use of the Premises may include a requirement that all materials, wastes or equipment with the potential to pollute urban runoff be stored in a manner that either prevents contact with rainfall and stormwater, or contains contaminated runoff for treatment and disposal. Licensee's is required to, and shall use, operate, maintain, develop, redevelop and retrofit the Premises, as necessary, in accordance with Stormwater Laws restricting the discharge of non-stormwater at or from the Premises; and Stormwater Laws requiring pollution prevention measures, source control measures, or the installation or use of BMPs. Licensee shall develop, install, implement and/or maintain at Licensee's sole cost and expense, any BMPs or similar pollution control devices required by Stormwater Laws and any implementing regulations or guidance.

Licensee understands and acknowledges that the Stormwater Laws applicable to Licensee's use of the Premises may be changed from time to time by federal, state and/or local authorities, and that additional requirements may become applicable based on changes in Licensee's activities or development or redevelopment by Licensee's or County. Licensee shall conduct stormwater training and perform regular stormwater self-

inspections, and maintain records of all stormwater training and self-inspections and provide all necessary documentation to County upon request.

Licensee shall develop, install, implement, and maintain any additional BMPs and/or other pollution control practices at the Premises at Licensee's sole cost and expense. To the extent there is a conflict between any federal, state or local law, Licensee shall comply with the more restrictive provision. If County receives any fine or fines from any regulatory agency as a result of Licensee's failure to comply with Stormwater Laws, Licensee shall reimburse County for the entire amount of the fine(s).

13. Hazardous Substances. Licensee shall be solely responsible for fully complying with all present or future federal, state and local laws, statutes, regulations, ordinances, policies, guidelines and orders of any governmental entity regarding contaminated soils, hazardous materials or environmental cleanup, regardless of whether or not the obligation to comply is an obligation of the land owner. If any hazardous substance spills, leaks or is discharged from any facility on the Premises, Licensee shall immediately make all repairs necessary to prevent further spills, leaks or discharges and shall immediately clean up and promptly dispose of the spilled hazardous substance and any soil contaminated by the spill. If the Licensee fails to make the required repairs, to clean up the spill or to properly dispose of any contaminated soil, County may after written notice to Licensee take all steps County deems necessary to make the necessary repairs, to clean up the spill and to dispose of any contaminated soil. The Licensee shall reimburse the County for the cost of all repair and cleanup work performed by the County. Licensee shall reimburse the County for the cost of any work, plus administrative expenses, within thirty (30) days of receiving a bill for the work from the County. Licensee shall be solely responsible for paying all fines, damages and penalties imposed by any governmental agency regarding the production, storage, distribution, processing, handling, disposing, spilling, leaking or discharging of any hazardous substance.

Licensee shall indemnify, defend, reimburse and hold harmless County, its elected officials, officers, employees and agents from any and all liability, claims, damages or injuries to any person, including injury to the County or any of County's elected officials, officers, employees, agents, representatives, guests, licensees, invitees, patrons, or of any other person, and all expenses of investigating and defending against all liability, claims, damages or injuries, arising from or alleged to have arisen from or in connection with the presence of hazardous substances, toxic materials or hazardous waste upon, about or beneath the Premises or migrating to or from the Premises or arising in any manner out of the violation of any governmental regulation pertaining to hazardous substances, toxic materials or hazardous waste which condition exists after the execution of this License.

14. Assignment. Licensee shall not assign or transfer any interest in this License.

15. Notices. Any notice required or permitted to be given pursuant to this License shall be written and shall be effective (a) when personally delivered to the recipient or sent by facsimile transmission; or (b) on the third business day after being sent by the United States Postal Service, postage prepaid and addressed to the party as follows:

If to County: County of San Diego
Department of General Services
Real Estate Services Division
5560 Overland Avenue
Suite 410
San Diego, California 92123

AND

As required by the notice provisions of the Information Technology and Telecommunications Service Agreement between the County of San Diego and Peraton Enterprise Solutions LLC dated November 15, 2016.

16. Entire Agreement. This License and any exhibits attached to this License constitutes the entire agreement between County and Licensee with respect to the License Premises. All other representations, oral or written, are superseded by this License. Neither party is relying on any representation outside of this License. This License may be changed only by written amendment signed by County and Licensee.

17. Interpretation. This License shall be governed by the laws of the State of California. However, the provisions of this License shall be strictly construed against Licensee.

18. Corporation in Good Standing. If Licensee is a California corporation, Licensee warrants that it is a corporation in good standing and is currently authorized to do business in California.

19. Authority to Sign. Licensee represents and warrants that it has full power and authority to execute and fully perform its obligations under this License without the need for any further action, and that the person executing this License on behalf of Licensee is the duly designated agent of Licensee and is authorized to act on behalf of Licensee.

THE REMAINDER OF THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK
THE SIGNATURE PAGE IS ON THE FOLLOWING PAGE

SIGNATURES

County and Licensee have caused this License to be executed by their duly authorized representatives.

"County"

County of San Diego,
a political subdivision of the State of California

By: _____
Marko Medved PE, CEM Director,
Department of General Services

"Licensee"

By: _____
Max Pinna
Peraton Enterprise Solutions LLC

EXHIBIT "A"

DESCRIPTION OF PREMISES

END OF SCHEDULE

Schedule 10.1.1 — Contractor Key Personnel

Table of Contents

1. Overview 3

2. Key Personnel.....3

1. OVERVIEW

Schedule 10.1.1 – Contractor Key Personnel describes the primary functions for each key position. The personnel filling key positions shall be deemed to be Key Personnel for the purposes of this Agreement. A list of the Key Personnel shall be maintained in the Standards and Procedures Manual.

2. KEY PERSONNEL

Key Personnel	High Level Description
Account Executive	Serves as the County's single point of contact with the Contractor and is responsible for the successful execution of the Agreement. The Account Executive must be knowledgeable about the County's business and the Services. The Account Executive works closely with the County Chief Information Officer (CIO) to ensure that the Services are aligned with the County's goals and expectations. All other Key Personnel listed in this Schedule must directly or indirectly report to the Account Executive.
Deputy Account Executive	Works closely with the Account Executive in executing the Agreement. The Deputy Account Executive must be knowledgeable about the County's business and the Services.
Enterprise Service Delivery Manager (SDM)	Oversees and manages operational delivery of IT and Telecommunication Services to the County. Oversees the activities of all Service Delivery Managers to ensure consistently high service performance across the County.
FG3 Service Delivery Manager (SDM)	Oversees the delivery of IT and Telecommunication Services to FG3. The FG3 SDM ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The FG3 SDM must have the authority to escalate across frameworks and secure resources as needed for IT and Telecommunication issues. The FG3 Service Delivery Manager works closely with the FG3 Group Information Technology Manger and Departmental IT staff.
HHSA Service Delivery Manager (SDM)	Oversees the delivery of IT and Telecommunication Services to HHSA. The HHSA SDM ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The HHSA SDM must have the authority to

Key Personnel	High Level Description
	escalate across frameworks and secure resources as needed for IT and Telecommunication issues. The HHSA SDM works closely with the HHSA Group Information Technology Manger and Departmental IT staff.
PSG Service Delivery Manager (SDM)	Oversees the delivery of IT and Telecommunication Services to PSG. The PSG SDM ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The PSG SDM must have the authority to escalate across frameworks and secure resources as needed for IT and Telecommunication issues. The PSG SDM works closely with the PSG Group Information Technology Manger and Departmental IT staff.
LUEG Service Delivery Manager (SDM)	Oversees the delivery of IT and Telecommunication Services to LUEG. The LUEG SDM ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The LUEG SDM must have the authority to escalate across frameworks and secure resources as needed for IT and Telecommunication issues. The LUEG SDM works closely with the LUEG Group Information Technology Manger and Departmental IT staff.
Special Service Levels Service Delivery Manager (SDM)	Oversees Special Service Level (SL) Requirements as defined in Exhibit 4.8.1 – Special Service Level Requirements of the Agreement, emergency and/or disaster related incidents, Board of Supervisors meetings, and support for the Clerk of the Board, Chief Administrative Office, and Board of Supervisors Offices. The Special SL SDM must have the authority to escalate across frameworks and secure resources as needed for IT and Telecommunication issues. The Special SL SDM will report to the representative of the County Technology Office (CTO) responsible for managing the SDMs. If there is an overlap period between Special SL support periods, the Contractor shall assign another resource(s) such that each active Service Request for Special SL support has a dedicated resource for the coordination and management of activities.

Key Personnel	High Level Description
	During periods when there are no active Service Requests for Special SL support, the CTO representative will direct the Special SLs SDM on other important activities and will also perform the responsibilities of the SDM as assigned by the Enterprise SDM.
Contracts Manager	Oversees the delivery of Contract Management Services. The Contracts Manager must be knowledgeable about the County's business and the Services. The Contracts Manager ensures consistently high performance in Contracts and Acquisition Services, monitors service delivery and evaluates feedback to develop quality improvement processes.
Chief Information Security Officer (CISO)	The CISO is responsible for aligning security initiatives, architectures, processes, and service delivery with enterprise programs and business objectives, ensuring that information assets and technologies are adequately protected. The Contractor CISO works closely with the County's CISO in identifying, developing, implementing, and maintaining security-related processes that reduce the organization's operational risks.
Chief Technology Architect (CTA)	The CTA is responsible for providing principles, best practices, innovation, market trends, and future-looking models for the County's IT infrastructure; and serving as a bridge for all the architecture groups and areas as described in Schedule 4.3 for the CTA. The Contractor CTA works closely with the County's CTA to oversee and coordinate the top-down approach to managing and sharing data, systems, and processes.
Cross Functional Services Manager	Oversees the delivery of Cross Functional Services. The Cross Functional Services Manager ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The Cross Functional Services Manager ensures integration and consistency across Service Frameworks and functional resources to deliver quality service.
Service Desk Manager	Oversees the delivery of Service Desk Services. The Service Desk Manager ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement

Key Personnel	High Level Description
	processes. The Service Desk Manager must have the authority to escalate and secure resources as needed to resolve issues.
End User Services Manager	Oversees the delivery of End User Services. The End User Services Manager ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The End User Services Manager must have the authority to escalate and secure resources as needed to resolve issues.
Network Services Manager	Oversees the delivery of Network Services. The Network Services Manager ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The Network Services Manager must have the authority to escalate and secure resources as needed to resolve issues.
Data Center Services Manager	Oversees the delivery of Data Center Services. The Data Center Services Manager ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The Data Center Services Manager must have the authority to escalate and secure resources as needed to resolve issues.
Enterprise Applications Services Manager	Oversees the delivery of Applications Development and Maintenance and Operations Services. The Applications Services Manager ensures consistently high service performance, monitors service delivery and evaluates feedback to develop quality improvement processes. The Applications Services Manager must have the authority to escalate and secure resources as needed to resolve issues.
Project Management Office (PMO) Manager	The PMO Manager is responsible for ensuring the consistency, predictability, efficiency, and effectiveness of the Contractor's project delivery capability. The PMO Manager provides leadership in best practices and is highly customer-focused.
Transition Services Manager	Oversees the delivery of Transition Services. The Transition Services Manager oversees the transition from the Legacy Provider to the Contractor while ensuring consistently high service performance, monitoring service delivery and evaluating feedback to develop quality improvement processes. The Transition Services Manager must have the authority to escalate and secure resources as needed to resolve issues.

Key Personnel	High Level Description
Enterprise Application Architect (EAA)	The EAA is responsible for leading the improvement of application quality, integration, and cost-effectiveness. This includes reviewing business and technical requirements, focusing on solution development throughout the project lifecycle, establishing and maintaining data standards, enterprise taxonomies, information management strategies and overall efforts to continuously improve the provision of Services in the EAA's areas of responsibility and areas as described in Schedule 4.3 for the EAA. The Contractor EAA works closely with the County's CTA in the governance and oversight of all application development across the enterprise and will act as a standing member of the Enterprise Architecture Governance Group.
Innovation Officer (IO)	The IO is responsible for driving continuous innovation and transformation of County services and leading the Innovation Management Services Office. This innovation leverages information technology, but is led from a business perspective. The IO will work directly with the County CTA in the governance and oversight of innovation and transformation initiatives. The IO will establish the charter, governance model and dev/ops agile environment to provide rapid prototyping of new business concepts and technology to determine feasibility and predict business outcome. The IO will meet with County business to determine concepts for innovation and will develop innovation based on functional business needs first. A full understanding of emerging business trends and technologies will be core responsibilities of the IO with additional responsibilities outlined in Schedule 4.3.

END OF SCHEDULE

Schedule 10.3 — Relationship Management

Table of Contents

1. Overview 3

2. High Level Requirements 3

3. Relationship Counterpart 4

4. Relationship Management Roles and Responsibilities 4

1. OVERVIEW

This Schedule 10.3 (Relationship Management) sets forth the roles and responsibilities of the entities for the relationship management ("Relationship Management") provided under the Agreement as part of the Services. Relationship Management are the activities, as further detailed in this Schedule 10.3, required to support County's overall relationship with the Contractor.

County recognizes that Relationship Management Services are an essential component for successful contract management and ongoing County - Contractor relationship satisfaction. County requires a relationship with Contractor based on the following key ingredients, including:

- Mutual trust and respect
- Excellent communication between both Entities
- Well-defined objectives and service levels
- Appropriate governance structures
- Well-defined roles and responsibilities

2. HIGH LEVEL REQUIREMENTS

The Contractor relationship management team will work with the County team to achieve a number of County relationship goals and objectives, including:

- Delivery of high-quality IT and telecommunication services to support County business needs
- Continued high customer satisfaction from all technical and operational End-Users of Services
- Continuous recommendation of improvements to the functionality, creation and delivery of Services—to the extent that County business objectives would be better served
- Development of the business rationale and benefits of any proposed changes and communicate these to the team and other County stakeholders, as appropriate
- Working within the mutually-agreed upon structure regarding processes and procedures
- Assisting County in its planning activities as required
- Ensuring sufficient and continued communication

The following are additional County and Contractor relationship management functions that are essential to managing the relationship:

- Financial management
- Performance management
- Contract management

3. RELATIONSHIP COUNTERPART

The following table defines the hierarchy and relationship counterpart by County and Contractor roles.

County of San Diego	Contractor
Chief Administrative Officer	Executive Vice President & General Manager
Assistant Chief Administrative Officer	Vice President of State, Local and Education, U.S. Public Sector
Chief Information Officer	Account Executive
CTO Contract Manager	Contracts Manager

4. RELATIONSHIP MANAGEMENT ROLES AND RESPONSIBILITIES

Relationship Management Roles and Responsibilities		
Strategy and Planning	**Contractor**	**County**
1. Provide Contractor with County strategic business and technology imperatives that require Contractor support.		X
2. Recommend services, technologies and/or products to County's IT management that add value to County.	X	
3. Review projects and project plans.	X	
4. Review and approve projects and project plans.		X
5. Develop strategic IT plan to support County strategic business plans.		X
6. Participate in the development of County strategic business plans, as requested by County.	X	
7. Develop/implement operational plans in accordance with authorized strategic IT plan, architecture and implementation strategies.	X	
8. Review and approve operational plans in accordance with authorized strategic IT plan, architecture and implementation strategies.		X
9. Provide IT research assistance on new technologies.	X	
10. Provide Business case assistance and preparation, as required.	X	

Relationship Management Roles and Responsibilities		
11. Provide IT solutions, expertise, and advisory services that are appropriately aligned with County's needs and business focus.	X	
12. Establish business criteria for all services, standards and delivery requirements.		X
13. Recommend appropriate Services, standards and procedures.	X	
14. Review and approve all recommended services, standards and procedures.		X
15. Adhere to County Policies and Standards.	X	
16. Develop, document and maintain Standards and Procedures Manual.	X	
17. Approve Standards and Procedures Manual.		X
18. Provide the Standards and Procedures Manual electronically (and in a manner such that it can be accessed via the Service Portal.	X	
19. Communicate to all End-Users the availability of and methodology for accessing the Standards and Procedures Manual.	X	
20. Develop Demand Management Report (DMR), which shall include forecasts of expected changes in Services demand.		X
21. Review and analyze DMR.	X	
22. Provide input to demand forecasts for DMR.	X	
23. Develop response to demands in the DMR.	X	
24. Develop and provide action plans as a result of review of DMR.	X	
25. Approve DMR action plans.		X
Contract Management	**Contractor**	**County**
26. Monitor contract terms, technology operations and management processes to ensure compliance.		X
27. Monitor and revise contracts as applicable and review recommended contract modifications provided by the other party.		X
28. Monitor and revise contracts as applicable and review recommended contract modifications provided by the other party.	X	
29. Provide data required to assess fee reductions and incentives.	X	
30. Identify and manage Contractor fee reductions, based on performance information and contract terms.		X
31. Approve changes.		X
32. Implement changes.	X	

Relationship Management Roles and Responsibilities		
33. Conduct regularly reviews of the risk exposure of the relationship and overall transaction between County and Contractor using a framework, which includes without limitation: • Security audit including access rights • Quality of service delivery • Delayed service delivery • Business continuity and disaster recovery • Non-performance or inability to deliver Services • Quality of the 'Relationship'		X
34. Participate in regular reviews of the risk exposure of the relationship and overall transaction between County and Contractor.	X	
Relationship Management	**Contractor**	**County**
35. Provide support and commitment of County executives to the relationship.		X
36. Provide support and commitment of Contractor executives to the relationship.	X	
Financial Management	**Contractor**	**County**
37. Establish, maintain and ensure an asset register for all assets relevant to the Services is being managed.	X	
38. Establish, maintain and ensure a contract register for all contracts relevant to the Services is being managed.	X	
39. Review asset register and contract register.		X
40. Provide Contractor data to a third-party benchmarking vendor for use in conducting periodic cost and performance benchmark comparison upon request.	X	
41. Monitor and manage financial administration practices and procedures associated with the Agreement.		X
42. Provide data in order to conduct charge back per County requirements.	X	
43. Identify billing disparities and work with Contractor to identify corrective actions.		X
44. Implement corrective actions for billing disparities.	X	
45. Provide a monthly report of Services consumed and any variances to plan.	X	

Relationship Management Roles and Responsibilities		
46. Maintain an audit trail and records of all costs incurred under the Agreement and net book value for assets.	X	
47. Proactively ensure that all unnecessary costs are eliminated, and that costs are managed in an efficient manner.	X	
48. Approve all cost controls.		X
49. Maintain full records of assets (including ownership) used to support the delivery of Services under the Agreement and upon request, make such records available to County for review.	X	
Service Level Management	**Contractor**	**County**
50. Manage and coordinate all delivery aspects of the Services.	X	
51. Provide periodic written performance management reports to County on Service Levels (SLs) and conduct periodic scheduled and ad hoc review meetings as required.	X	
52. Review and monitor Contractor performance against SLs, return-on-investment metrics, performance improvement plans and industry benchmarks.		X
53. Ensure Contractor understanding of and adherence to SLs and any implementations of required changes to achieve such SLs.	X	
54. Ensure in-scope technical solutions are consistent with County's business strategy and architecture.	X	
55. Ensure Contractor performance meets business requirements.	X	
56. Conduct a formal review and report on root causes of service delivery or other relationship related matters, and document such findings.	X	
Resource Management	**Contractor**	**County**
57. Ensure that staffing, technology and skill levels are adequate to achieve contract objectives.	X	
58. Inform County of any potential Key Personnel staffing changes and of any new personnel assignments planned for new projects and Services.	X	
59. Review and authorize Key Personnel changes to existing Services and personnel for new projects and Services.		X
60. Define any constraints for the use of subcontractors.		X
61. Provide Contractor staff turnover data when requested by County.	X	

Relationship Management Roles and Responsibilities		
62. Provide monthly an updated contractor organization chart related to roles supporting and/or delivering Service to the County.	X	
Integration Management	**Contractor**	**County**
63. Provide information on integration requirements.		X
64. Define integration solutions.	X	
65. Approve integration solutions.		X
66. Develop Operating Level Agreements (OLAs) between third-party Entities and Contractor if other third-party Contractors of Services are providing services that integrate or impact upon those defined in the Agreement.	X	
Customer Satisfaction Management	**Contractor**	**County**
67. Provide periodic written performance management reports to County on SLs and conduct periodic scheduled and ad-hoc review meetings as required.	X	
68. Conduct customer satisfaction survey.	X	
69. Participate in and review customer satisfaction survey.		X

END OF SCHEDULE

Schedule 12.1.1 – Information Privacy and Security, Criminal Offender Record Information, California Law Enforcement Telecommunication Systems, and County Facility Access

Table of Contents

1. Overview....3

2. Business Associate Agreement....5

3. Privacy and Security of Personal Information and Personally Identifiable Information 12

4. Data Security Requirements 16

5. CORI/CLETS Requirements 24

6. Personnel Access 29

7. Miscellaneous 31

1. OVERVIEW

A. This Schedule 12.1.1 is intended to protect the privacy and security of specified County information that Contractor may receive, access, store, maintain or transmit, under this Agreement, and to comply with the applicable federal and State laws and regulations governing the access, use and disclosure of the specified County information. The County information subject to the requirements of this Schedule consists of:

1. Protected Health Information (PHI), as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and
2. Personal Information (PI) as defined under the California Civil Code Section 1798.3. PI may include data provided to the County by the State of California or by the Social Security Administration (SSA); and
3. Personally Identifiable Information (PII) as defined under the Information Exchange Agreement (IEA) between the State of California and the SSA dated October 11, 2014, which incorporates the Computer Matching and Privacy Protection Agreement (CMPPA) between the SSA and the State of California's Health and Human Services Agency dated July 2, 2014; and
4. Criminal Offender Record Information (CORI) as defined by California Penal Code sections 11075 and 13102, including information from the California Law Enforcement Telecommunications System (CLETS), the County of San Diego Probation Case Management System (PCMS), and local County records.
5. This Schedule does not reduce any other obligation set forth in the Agreement or any other law or regulation governing the information. To the extent another provision of the Agreement requires different protection of information subject to the requirements of this Schedule, the provisions requiring greater protection of the information shall prevail.

B. This Schedule consists of the following parts:

1. Section 1, Business Associate Agreement;
2. Section 2, Privacy and Security of PI and PII;
3. Section 3, Data Security Requirements; and
4. Section 4, CORI/CLETS; and
5. Section 5, Miscellaneous.

C. Definitions: Capitalized terms used in this Section 1, and for which no definition in this Section 1 is provided, shall be defined as otherwise defined in the Agreement. Terms used, but not otherwise defined, in this Section 1 shall have the same meaning as those terms as are defined in 45 Code of Federal Regulations (CFR) section 160.103 and 164.501. (All regulatory references in this BAA are to Title 45 of the CFR unless otherwise specified.)

1 "Breach"

1.2 For Sections 1 and 2 of this Exhibit 12.1.1, "Breach" shall have the same meaning given to such term under HIPAA.

1.3 For purposes of Section 3 of this Exhibit 12.1.1, "Breach" "Breach" shall have the same meaning given to such term under the IEA and CMPPA. It shall include a "PII loss," as defined in the CMPPA, and both a "Breach of the security of the system" and a "Notice Triggering Personal Information" event, as identified in CIPA (Civil Code section 1798.29).

2 "Business Associate" shall have the same meaning as the term under HIPAA, and for purposes of this Agreement, shall mean the Contractor. "Contractor Employees" shall mean, for purposes of this Schedule 12.1.1, Contractor's officers, directors, employees, volunteers and interns.

3 "CORI" shall mean records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release (Cal. Pen. Code sections 11075 and 13102). CORI includes but is not limited to information from the CLETS, PCMS, and local County records.

4 "County Hybrid Entity" shall mean that part of County designated as the hybrid entity subject to the Standards for Privacy of Individually Identifiable Health Information set forth in sections 160 and Part 164, Subparts A and E and those parts of County designated as business associates of other entities subject to the Standards for Privacy of Individually Identifiable Health Information set forth in Parts 160 and 164, Subparts A and E.

5 "County PHI" shall have the same meaning as "Protected Health Information" (PHI) below, specific to PHI received from, or accessed, created, stored, maintained, transmitted, used, disclosed, or received by Contractor, or its subcontractors and agents, on behalf of County, under this Agreement.

6 "County PII/PI" shall have the same meaning as Personally Identifiable Information/Personal Information as below, specific to PII/PI received by Contractor from County or acquired or created by Contractor in connection with performing the functions, activities, and services specified in this Section 2 on County's behalf.

7 "Covered Entity" shall generally have the same meaning as the term "covered entity" at section 160.103, and for purposes of this BAA, shall mean County-Hybrid Entity.

8 "HIPAA" means collectively the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005, 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164.

9 "Individual" shall have the same meaning as the term ''individual'' in section 164.501 and shall include a person who qualifies as a personal representative in accordance with section 164.502(g).

10 "Personal Information" shall have the same meaning given to such term in CIPA, section 1798.3(a).

11 "Personally Identifiable Information" (PII) shall have the same meaning given to such term in the IEA and the CMPPA.

12 "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in section 164.501 and is limited to information created or received by Contractor from or on behalf of County.

13 "Required by law" shall have the same meaning as the term ''required by law'' in section 164.501.

14"Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

15 "Security incident" means the attempted and successful unauthorized access, use, disclosure, modification, or destruction of County PHI, County PI or PII, confidential data, or interference with system operations in an information system that processes, maintains or stores County PHI.

16 "Unsecured PHI" shall have the meaning given to such term under HIPAA and, 42 U.S.C., section 17932(h), and any guidance issued pursuant to such regulations.

2. BUSINESS ASSOCIATE AGREEMENT

2.1. Recitals

2.1.1. This Section 1, Business Associate Agreement ("BAA") constitutes a Business Associate relationship as that term is defined and used in HIPAA.

2.1.2. The County may, from time-to-time, disclose to the Contractor certain information pursuant to the terms of this BAA, some of which may constitute PHI, including PHI in electronic media under federal law.

2.1.3. As set forth in this BAA, Contractor, hereafter, is the Business Associate of County, acting on County's behalf and providing services, or performing or assisting in the performance of activities on County's behalf, which may include accessing, creation, receipt, storing, maintenance, transmittal, use or disclosure of PHI.

2.2. Contractor Responsibilities

2.2.1. General Obligations

2.2.2. Permitted Uses and Disclosures of County PHI by Contractor. Contractor shall only use County PHI as required by the Agreement or as required by law. Any such use or disclosure shall, to the extent practicable, be limited to the limited data set as defined in section 164.514(e)(2), or if needed, to that which is minimally necessary to accomplish the intended purpose of such use or disclosure in compliance with HIPAA.

2.2.3. Except as otherwise limited in this Agreement, Contractor may use or disclose County PHI on behalf of, or to provide services to, County for the purposes set forth in the Agreement, if such use or disclosure of PHI would not violate HIPAA if done by County.

2.2.4. Except as otherwise limited in the Agreement, Contractor may use County PHI to provide Data Aggregation services to County as permitted by sections 164.504(e)(2)(i)(B).

2.2.5. Prohibited Uses and Disclosures

2.2.6. Contractor shall not disclose County PHI to a health plan for payment or health care operations purposes if County PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the Individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and HIPAA.

2.2.7. Contractor shall not directly or indirectly receive remuneration in exchange for County PHI, except with the prior written consent of County and as permitted by 42 U.S.C. section 17935(d)(2).

2.2.8. Safeguards

2.2.8.1. Contractor shall comply with HIPAA regarding any and all operations conducted on behalf of County under this Contract and shall use appropriate safeguards that comply with HIPAA to prevent the unauthorized use or disclosure of County PHI.

2.2.8.2. Contractor shall develop and maintain a written information privacy and security program that complies with HIPAA, and that includes administrative, physical, and technical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

2.2.9. Security. Contractor shall ensure the continuous security of all computerized data systems and paper documents containing County PHI. These steps shall include, at a minimum:

2.2.9.1. Comply with all Standards put forth in Section 3, Data Security Requirements, of this Schedule 12.1.1;

2.2.9.2. Achieve and maintain compliance with HIPAA; and

2.2.9.3. Provide a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in federal agencies, and as otherwise required by the Agreement.

2.2.10. Mitigation of Harmful Effects. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PHI by Contractor, Contractor's Employees, Contractor's agents, Contractor's subcontractors or Contractor's vendor, and/or in violation of the requirements of the Contract.

2.2.11. Contractor's Agents, Subcontractors and Vendors. Contractor shall ensure that any agent, subcontractor or vendor to whom it provides County PHI, imposes the same conditions on such agents, subcontractors and vendors that apply to Contractor with respect to County PHI under this BAA, and that comply with all applicable provisions of HIPAA, including requirements that such agents, subcontractors and vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect County PHI. Contractor shall incorporate, when applicable, the relevant provisions of this BAA into each subcontract to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured County PHI be reported to Contractor.

2.2.12. In accordance with section 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by any agent, subcontractor or vendor of the agreement between Contractor and the agent, subcontractor and vendor, Contractor shall:

2.2.12.1. Provide an opportunity for the agent, subcontractor or vendor to end the violation and terminate the agreement if the agent, subcontractor or vendor does not end the violation within the time specified by County; or

2.2.12.2. Immediately terminate the agreement if the agent, subcontractor or vendor has violated a material term of the agreement and cure is not possible.

2.2.13. Availability of Information to County. Contractor shall provide access to County PHI at the request of County, in the time and manner designated by County, pursuant to section 164.526.

2.2.14. Contractor shall use the forms and processes developed by County for this purpose and shall respond to all requests for access to records requested by County within forty-eight (48) hours of receipt of such request by producing records or verifying that there are none.

2.2.15. Contractor shall make internal practices, books, and records relating to the use and disclosure of County PHI received from, or created or received by Contractor on behalf of County available to County, or at the request of County to the Secretary, in a time and manner designated by County or the Secretary.

2.2.16. Cooperation with County. Contractor shall cooperate and assist County to the extent necessary to ensure County's compliance with the applicable terms of HIPAA, such as, but not limited to:

2.2.16.1. Documentation of Disclosures. Contractor shall document disclosures of County PHI and make these disclosures available to County in accordance with HIPAA, including but not limited to sections 164.528, and 42 USC section 17935, and in the time and manner designated by County.

2.2.16.2. If Contractor maintained electronic health records as of January 2009, when requested, Contractor shall provide an accounting of disclosures including those for Treatment, Payment, and Healthcare Operations (TPO). If Contractor acquired electronic health records for County after January 1, 2009, or acquires electronic records for County, when requested, Contractor shall provide an accounting of disclosures, including those for TPO, effective with disclosures on or after the date the electronic health record was or is acquired, or on or after January 1, 2011, whichever date is later.

2.2.16.3. The electronic accounting of disclosures shall include the three (3) years prior to the request for an accounting. Contractor shall provide to County, in the time and manner designated by County, but no more than sixty (60) calendar days after County's request, an accounting of disclosures necessary to meet the requirements in section 164.528.

2.2.16.4. Reporting of Unauthorized Use or Disclosure. Contractor shall implement reasonable systems for the discovery of and prompt reporting to County of any use or disclosure of County PHI not allowed for by the Agreement and/or any transmission of unsecured County PHI. Contractor shall provide all reports of unauthorized uses or disclosures simultaneously to the COR and County Privacy Officer.

2.2.17. Initial Report

2.2.17.1. Contractor shall notify County COR and County Privacy Officer immediately by telephone call and by email upon the discovery of a breach of unsecured County PHI in electronic media or in any other media if County PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to County by the SSA.

2.2.17.2. Contractor shall notify County COR and County Privacy Officer by email within twenty-four (24) hours of the discovery of any suspected security incident, breach or loss of County PHI.

2.2.17.3. A suspected security incident or breach shall be treated as discovered by Contractor or its agent, subcontractor or vendor as of the first day the breach or security incident is known, even if it is not confirmed, or by exercising reasonable diligence would have known, to any person (other than the person causing or committing the security incident or breach) who is a Contractor Employee or agent, subcontractor or vendor of Contractor.

2.2.17.4. Reporting shall additionally include emailing to the County COR and County Privacy Officer of the "County Privacy Incident Report" form within twenty-four (24) hours of any above incident, to include all information known at the time of the notification. Contractor shall report using the form attached hereto as Exhibit 12.1.1-1.

2.2.17.5. Investigation and Investigation Report. Contractor shall immediately investigate such security incident, breach, or unauthorized access, use or disclosure of County PHI. Within seventy-two (72) hours of the discovery, Contractor shall submit an updated "County Privacy Incident Report" to County COR and County Privacy Officer.

2.2.17.6. Complete Report. Contractor shall provide a complete report of the investigation within five (5) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "County Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA and applicable federal and State law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. The report shall be submitted to the County COR and County Privacy Officer. If County requests information in addition to that listed on the "County Privacy Incident Report" form, Contractor shall make reasonable efforts to provide County with such information. County will review and, appropriate, approve the determination of whether a breach occurred, Individual notifications are required, and the corrective action plan is adequate. County action or inaction in determining whether a breach occurred, the need for notifications or any correction shall not relieve Contractor of any federal or State requirements with which Contractor must comply.

2.2.18. Responsibilities for Notification of Breaches. If County determines that the cause of a breach of County PHI is attributable to Contractor, Contractor Employees or Contractor's subcontractors, agents or vendors, Contractor shall notify Individuals of the breach or unauthorized use or disclosure when notification is required under federal or State law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirements that:

2.2.18.1. Notifications be made to Individuals without unreasonable delay and in no event later than sixty (60) calendar days from the date the breach was discovered. County shall approve the time, manner and content of any such notifications before notifications are made.

2.2.18.2. Notifications shall be made to media outlets and to the Secretary, if a breach of unsecured County PHI involves more than five-hundred (500) residents of the State of California or its jurisdiction. County shall approve the time, manner and content of any such notifications before notifications are made.

2.2.18.3. Nothing in this Schedule 12.1.1 shall limit or reduce Contractor's indemnification or other responsibilities set forth in the Agreement, nor shall anything in this Schedule 12.1.1 reduce or limit Contractor's liability to County or any third party as set forth in the Agreement.

2.2.18.4. Corrective Action. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PHI, Contractor shall take prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and any action pertaining to such unauthorized disclosure required by applicable federal and State laws and regulations.

2.2.19. Designation of Individuals

2.2.19.1. Contractor shall designate a privacy officer to oversee its data privacy program who shall be responsible for carrying out the requirements of this Agreement and for communicating on Privacy matters with County.

2.2.19.2. Contractor shall designate a security officer to oversee its data security program who shall be responsible for carrying out the requirements of this Agreement and for communicating on security matters with County.

2.2.20. County Responsibilities. County shall not request Contractor to use or disclose County PHI in any manner that would not be permissible under HIPAA if done by County.

3. PRIVACY AND SECURITY OF PERSONAL INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

3.1. Recitals

3.1.1. The purpose of this Section 2 of Schedule 12.1.1 is to set forth Contractor's Privacy and Security obligations with respect to PI and PII that the Contractor may access, create, receive, maintain, use, store or disclose for or on behalf of County pursuant to this Agreement. Specifically, this Section 2 applies to PI and PII that is not PHI, and therefore, is not addressed in Section 1, the Business Associate Agreement, of this Schedule 12.1.1. To the extent that data is both PHI and PI, or both PHI and PII, both Sections 1 and 2 of this Schedule 12.1.1 govern its use.

3.1.2. The IEA requires County to extend the IEA's terms to contractors who receive data provided to County from the SSA, or data provided to County from the SSA through the State. If Contractor receives such data from County, Contractor must comply with the IEA.

3.2. Contractor Responsibilities

3.2.1. Permitted Uses and Disclosures of County PII/PI by Contractor. Contractor shall only use County PII/PI to perform functions, activities, or services for or on behalf of County pursuant to this Agreement, provided that such use or disclosure does not violate any applicable federal or State law or regulation.

3.2.2. Confidentiality of Alcohol and Drug Abuse records. Contractor shall comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter 1, Subchapter A, Part 2, as applicable.

3.2.3. Prohibited Uses and Disclosures. Contractor shall not use or disclose County PII/PI, other than as permitted or required by the Agreement or as permitted or required by law.

3.2.4. Safeguards

3.2.4.1. Contractor shall use appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of County PII/PI and to prevent use or disclosure of County PII/PI, other than as provided for by the Agreement.

3.2.4.2. Contractor shall develop and maintain a written information privacy and security program that includes administrative, physical, and technical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities.

3.2.5. Security. Contractor shall take any and all steps necessary to ensure the continuous safety of all data systems containing County PII/PI. The Contractor shall, at a minimum:

3.2.5.1. Comply with all of the data system security precautions listed in Section 3 of this Schedule 12.1.1, Data Security Requirements; and

3.2.5.2. Provide a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

3.2.5.3. Provide a level and scope of security that is no less than otherwise provided by the Agreement; and

3.2.5.4. If the data includes County PII, Contractor shall also comply with the Privacy and Security requirements in the CMPPAA and the IEA.

3.2.6. Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PII/PI by Contractor or its agents, in violation of this Schedule 12.1.1.

3.2.7. Contractor's Employees, Agents, Subcontractors and Vendors. Contractor shall ensure that any Contractor Employee, agent, subcontractor or vendor that accesses, creates, receives, maintains, stored, uses, discloses, receives or transmits County PII/PI on behalf of the Contractor shall adhere to the same restrictions, conditions, and requirements that apply to the Contractor. Contractor shall incorporate, when applicable, the relevant provisions of this Schedule 12.1.1 into each subcontract or sub-award to such agents, subcontractors and vendors, including the requirements related to security incidents or breaches of unsecured County PII/ PI.

3.2.8. Availability of Information. Contractor shall make County PII/PI available to County for purposes of oversight, inspection, amendment, and response to request for records, injunctions, judgments, and orders for production of County PII/PI. Contractor shall provide a list of all Contractor Employees, subcontractors, vendors and agents who have access to County PII/PI, including employees, agents and vendors of its subcontractors, agents and vendors, at the request of County. Contractor shall provide any requested records to County within forty-eight (48) hours of such request.

3.2.9. Internal Practices. Contractor shall make internal practices, books, and records relating to the use and disclosure of County PII/PI received from, or created or received by Contractor on behalf of County available to County, in a time and manner designated by County. Confidentiality shall not prevent County, its agents, or any other governmental entity from accessing such records if that access is legally permissible under the applicable federal or State regulations.

3.2.10. Cooperation with County. Contractor will cooperate and assist County, in the time and manner designated by County, to ensure County's compliance with applicable federal and State laws and regulations, such as, but not limited to CIPA. Contractor's cooperation shall include, but is not limited to: accounting of disclosures, correction of errors, production, disclosures of a security breach, and notice of such breach to affected individuals that involve County PII/PI and Contractor.

3.2.11. Reporting of Breaches and Security Incidents. Contractor shall implement reasonable systems for the discovery of, prompt reporting to County of, and prompt corrective action regarding any use or disclosure, or suspected use or disclosure, of County PII/PI not provided for by the Agreement and/or any transmission of unsecured County PII/PI and shall take the following steps:

3.2.11.1. Contractor shall make all reports required by this Section 2 of breaches and security incidents simultaneously to County COR and County Privacy Officer.

3.2.11.2. Initial Reporting

3.2.11.2.1. Reporting shall be immediate, by both telephone and email, upon the discovery of a breach of unsecured County PII/PI in electronic media or in any other media if County PII/PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to County by the SSA.

3.2.11.2.2. Reporting shall be within twenty-four (24) hours by email of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of County PII/ PI in violation of this Section 2, or potential loss of confidential data affecting this Section 2.

3.2.11.2.3. A breach or suspected security incident shall be treated as discovered by Contractor as of the first day on which the breach is known, even if not confirmed, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of the Contractor.

3.2.11.2.4. Reporting shall additionally include emailing of the "County Privacy Incident Report" form within twenty-four (24) hours of any above incident, to include all information known at the time of the notification. Contractor shall use the form attached hereto as Exhibit 12.1.1-1. Investigation and Investigation Report. Contractor shall immediately investigate such security incident or breach. Within seventy-two (72) hours of the discovery, Contractor shall submit an updated "County Privacy Incident Report."

3.2.11.2.5. Complete Report. Contractor shall provide a complete report of the investigation within five (5) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "County Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of federal and State law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If County requests information in addition to that listed on the "County Privacy Incident Report" form, Contractor shall make reasonable efforts to provide County with such information. County will review and approve the determination of whether: a breach occurred, individual notifications are required, and the corrective action plan is adequate.

3.2.11.2.6. Responsibility for Reporting Breaches. If County determines that the cause of a breach of County PII/PI is attributable to Contractor, Contractor Employees, or Contractor's subcontractors, agents or vendors, Contractor is responsible for all required reporting as specified under CIPA section 1798.29(a) and as may be required under IEA, as well as any other federal or State law and shall pay any costs of such notifications, as well as any costs associated with the breach. County shall approve the time, manner, and content of any such notifications and County's review and approval must be obtained before the notifications are made. If the Contractor believes duplicate reporting of the same breach or incident may occur, because its subcontractors or agents may report the breach or incident to County as well, Contractor shall notify County and may take action to prevent duplicate reporting.

3.2.12. Nothing in this Schedule 12.1.1 shall limit or reduce Contractor's indemnification or other responsibilities set forth in the Agreement, nor shall anything in this Schedule 12.1.1 reduce or limit Contractor's liability to County or any third party as set forth in the Agreement.

3.2.13. Corrective Action. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of County PII/PI, Contractor shall take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and any action pertaining to such unauthorized disclosure required by applicable federal and State laws and regulations.

3.2.14. Designation of Individuals. Contractor shall appoint Privacy and Security officials who are accountable for compliance with this Section 2 and for communicating Privacy and Security matters to County.

4. DATA SECURITY REQUIREMENTS

4.1. Contractor shall ensure the continuous security of all data systems and paper documents containing County PHI and/or County PII/PI. The security obligations set forth herein are in addition to those set forth in the Agreement, and shall not lessen or decrease Contractor's security obligations. These steps shall include, at a minimum:

4.2. Personnel Controls. Contractor shall ensure that all workforce members who assist in the performance of functions or activities on behalf of County, or access or disclose County PHI and/or County PII/PI, shall:

4.2.1. Have undergone a thorough Contractor background check, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security, privacy, or integrity of County PHI and/or County PII/PI, prior to the workforce member obtaining access to County PHI and/or County PII/PI. The Contractor shall retain each workforce member's Contractor background check documentation for a period of three (3) years following contract termination.

4.2.2. Complete privacy and security training, at least annually, at Contractor's expense. Each of Contractor's Employees, and Contractor's agents, subcontractors and vendors and their employees, who receive information privacy and security training shall sign a certification, indicating the person's name and the date on which the training was completed. These certifications shall be retained for a period of six (6) years following contract termination, and shall be available to County upon request.

4.2.3. Sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the workforce member prior to access to County PHI and/or County PII /PI and shall be renewed annually. The Contractor shall retain each person's written confidentiality statement for County inspection for a period of six (6) years following contract termination. The form of the Confidentiality Statement is attached hereto as Exhibit 12.1.1-2.

4.2.4. Be appropriately sanctioned if they fail to comply with security and privacy policies and procedures, including termination of employment when appropriate.

4.3. Physical Security Controls. Contractor shall safeguard County PHI and/or County PII/PI from loss, theft, inadvertent disclosure, and therefore shall:

4.3.1. Ensure County PHI and/or County PII/PI is used and stored in an area that is physically safe from access by unauthorized persons during both working hours and nonworking hours;

4.3.2. Secure all areas of Contractor facilities where Contractor workers use or disclose County PHI and/or County PII/PI. The Contractor shall ensure that these secured areas are only accessed by authorized individuals with properly coded key cards, authorized door keys or other access authorization, and access to premises is by official identification;

4.3.3. Issue Contractor Employees who assist in the administration of County PHI and/or County PII/PI identification badges and require Contractor Employees to wear badges at facilities where County PHI and/or County PII/PI is stored or used;

4.3.4. Ensure each location where County PHI and/or County PII/PI is used or stored has procedures and controls that ensure an individual whose access to the facility is terminated:

4.3.4.1. Is promptly escorted from the facility by an authorized Contractor Employee; and

4.3.4.2. Immediately has their access revoked to any and all County PHI and/or County PII/PI.

4.3.5. Ensure there are security guards or a monitored alarm system twenty-four (24) hours a day, seven (7) days a week at facilities where County PHI and/or County PII/PI is stored;

4.3.6. Ensure data centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of County PHI and/or County PII/PI have perimeter security and access controls that limit access to only authorized Information Technology Staff. Visitors to the data center area must be escorted by authorized Contractor Employees at all times;

4.3.7. Store paper records with County PHI and/or County PII/PI in locked spaces in any facilities that are multi-use, meaning that there are County PHI and/or County PII/PI functions and Contractor functions in one building in work areas that are not securely segregated. The contractor shall have policies that state Contractor Employees shall not leave records with County PHI and/or County PII/PI unattended at any time in cars or airplanes and shall not check County PHI and/or County PII/PI on commercial flights; and

4.3.8. Use all reasonable means to prevent non-authorized personnel and visitors from having access to, control of, or viewing County PHI and/or County PII/PI.

4.4. Technical Controls. Contractor shall ensure that:

4.4.1. All workstations and laptops that process and/or store County PHI and/or County PII/PI shall:

4.4.1.1. Be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution shall be full disk; and

4.4.1.2. Install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

4.4.1.3. Apply critical security patches. There shall be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. All applicable patches shall be installed within thirty (30) days of vendor release.

4.4.1.4. All servers containing unencrypted County PHI and/or County PII/PI shall have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

4.4.1.5. Only the minimum necessary amount of County PHI and/or County PII/PI required to perform necessary business functions may be copied, downloaded, or exported.

4.4.1.6. All electronic files that contain County PHI and/or County PII/PI shall be encrypted when stored on any removable media or portable device (i.e. flash drives, cameras, mobile phones, CD/DVD, backup media, etc). Encryption shall be a FIPS 140-2 certified algorithm, which is 128bit or higher, such as AES.

4.4.1.7. All users shall be issued a unique user name for accessing County PHI and/or County PII/PI. Username shall be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours.

4.4.1.8. Passwords shall be:

4.4.1.8.1. At least eight characters;

4.4.1.8.2. A non-dictionary word;

4.4.1.8.3. Changed at least every ninety (90) days;

4.4.1.8.4. Changed immediately if revealed or compromised; and

4.4.1.8.5. Composed of characters from at least three of the following four groups from the standard keyboard:

4.4.1.8.6. Upper case letters (A-Z)

4.4.1.8.7. Lower case letters (a-z)

4.4.1.8.8. Arabic numerals (0-9)

4.4.1.8.9. Non-alphanumeric characters (punctuation symbols)

4.4.1.9. Passwords shall not be shared and shall not be stored in readable format on the computer.

4.4.1.10. Appropriate management control and oversight, in conjunction with County of the function of authorizing individual user access to County PHI and/or County PII/PI and over the process of maintaining access controls numbers and passwords.

4.4.1.11. When no longer needed, all County PHI and/or County PII/PI shall be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88.

4.4.1.12. All systems providing access to, transport of, or storage of County PHI and/or County PII/PI shall:

4.4.1.12.1. Provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

4.4.1.12.2. Display a warning banner stating: i) that the data that may be accessed is confidential, ii) that the systems accessed are logged, and iii) that authorized users' use of PHI/PII/PI data is exclusively for County business purposes. Users must be directed to log off the system if they do not agree with these requirements. If County provides a warning banner to be implemented by Contractor, Contractor's implementation shall satisfy this requirement except to the extent that Contractor is otherwise obligated to provide a warning banner for its business purposes.

4.4.1.12.3. Maintain an automated audit trail that identifies the user or system process which initiates a request for County PHI and/or County PII/PI, or which alters County PHI and/or County PII/ PI. The audit trail shall be date and time stamped, shall log both successful and failed accesses, shall be read only, and shall be restricted to authorized users. If County PHI and/or County PII/ PI is stored in a database, database logging functionality shall be enabled. Audit trail data shall be archived for at least three (3) years after occurrence, and shall be available to County upon request.

4.4.1.12.4. Use role based access controls for all users, enforcing the principle of least privilege.

4.4.1.12.5. Be protected by a comprehensive intrusion detection and prevention solution if they are accessible via the internet.

4.4.1.12.6. All data transmissions of County PHI and/or County PII/PI outside the secure internal network shall be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing County PHI and/or County PII/PI can be encrypted. This requirement pertains to any type of County PII/PI in motion such as website access, file transfer, and E-Mail.

4.5. Audit Controls. Contractor shall ensure:

4.5.1. All systems processing and/or storing County PHI and/or County PII/PI shall have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

4.5.2. All systems processing and/or storing County PHI and/or County PII/PI shall have a routine procedure in place to review system logs for unauthorized access.

4.5.3. All systems processing and/or storing County PHI and/or County PII/PI shall have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4.5.4. Investigate anomalies in usage of County PHI and/or County PII/PI identified by County and report conclusions of such investigations and remediations to County.

4.6. Business Continuity / Disaster Recovery Controls

4.6.1. Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of electronic County PHI and/or County PII/PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

4.6.2. Contractor shall ensure Data Centers with servers, data storage devices, and critical network infrastructure involved in the use or storage of County PHI or PII/PI, must include sufficient environmental protection such as cooling, power, fire prevention, detection, and suppression.

4.6.3. Contractor shall have established documented procedures to backup County PHI and/or County PII/PI to maintain retrievable exact copies of County PHI and/or County PII/PI. The plan shall include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore County PHI and/or County PII/PI should it be lost. At a minimum, the schedule shall be a weekly full backup and monthly offsite storage of County data.

4.7. Paper Document Controls. Contractor shall ensure:

4.7.1. County PHI and/or County PII/PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or separate office inside a larger office. Unattended means that information is not being observed by an employee authorized to access the information. County PHI and/or County PII/PI in paper form shall not be left unattended at any time in vehicles and shall not be checked in baggage during commercial flights.

4.7.2. Visitors to areas where County PHI and/or County PII/PI are contained shall be escorted and County PHI and/or County PII/PI shall be kept out of sight while visitors are in the area.

4.7.3. County PHI and/or County PII/PI shall be disposed of through confidential means, such as cross cut shredding and pulverizing.

4.7.4. County PHI and/or County PII/PI shall not be removed from the premises of the Contractor except for identified routine business purposes or with express written permission of County.

4.7.5. Faxes containing County PHI and/or County PII/PI shall not be left unattended and fax machines shall be in secure areas. Fax cover sheets shall contain a confidentiality statement instructing persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

4.7.6. Mailings of County PHI and/or County PII/PI shall be sealed and secured from damage or inappropriate viewing of County PHI and/or County PII/PI to the extent possible. Mailings which include 500 or more individually identifiable records of County PHI and/or County PII/PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of County's Privacy Officer to use another method is obtained.

4.7.7. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of County PHI and/or County PII/PI by Contractor or its agents, including a subcontractor, and/or in violation of the requirements of the Agreement.

5. CORI/CLETS REQUIREMENTS

5.1. Application. This Section 4, CORI/CLETS Requirements, applies to all Contractor employees, agents and subcontractors with access or potential access to CORI systems including those individuals with only unescorted access to County facilities/properties that store, process or transmit CORI/CLETS information in order to ensure the safety of program offenders and the integrity of this program. Access, or potential access to CORI/CLETS, can be in the form of hardcopy documentation, verbal communication, or other forms of information sharing, as well as access to Probation's facilities where CORI/CLETS is created, stored, handled or discussed.

5.2. Training Requirements. Contractor shall ensure that all Contractor Employees, agents and subcontractors, with physical and logical access to CORI and/or the facilities that secure CORI systems (unless these individuals are escorted by authorized personnel at all times) shall receive CORI/CLETS training from a certified CLETS/National Crime Information Center (NCIC) within six (6) months of assignment to this Agreement and biennially thereafter, in accordance with FBI Criminal Justice Information Services Security Policy (FBI CJIS) section 5.2 and California CLETS Policies, Practices and Procedures (PPP)section 1.8.3.A.4. CORI/CLETS training, which will include laws, policies, and consequences regarding access to, and use of, criminal offender record information, will be provided by the Probation Department if needed.

5.3. Training Reporting. A list of all persons with "physical and logical" access to CORI, his or her title, e-mail address and phone number(s) must be sent to the COR with the person's last date of training. Contractor shall complete the CORI/CLETS Training Request Form (Exhibit 12.1.1-2) for all employees, agents, volunteers, and subcontractors that have not received CORI/CLETS training or are required to renew his or her training. Contractor shall forward this list and form, within 30 days of employee, agent, volunteer and/or subcontractor assignment, to the Probation Department, 9444 Balboa Avenue, Suite 500, San Diego, CA 92123 Attention: Contracts Unit.

5.4. CORI/CLETS Clearance Requirements. In addition to the background check requirements of the Agreement, Contractor shall ensure that background checks are required and completed by all Contractor Employees, subcontractors, agents and vendors with access to CORI/CLETS information, systems and its facilities as provided under section 5.12 of the FBI CJIS and section 1.9.2 of the PPP.

5.4.1. At a minimum, the following background checks shall be completed and approved prior to performance under this Agreement:

5.4.1.1. Criminal background clearance through the Probation Department (Background Division), State of California Department of Justice (DOJ) and Federal Bureau of Investigation (FBI);

5.4.1.1.1. Out-of-State Background Checks: Contractor shall request a "hard card" from Probation for each out-of-state Contractor Employee, Subcontractor, agent or vendor, and Probation will provide to Contractor a "hard card" from the FBI. Each individual shall take the "hard card" to a local law enforcement agency, get fingerprinted and submit the cards to Probation at the following location: 9444 Balboa Avenue, Suite 500, San Diego, CA 92123, Attn: Background Division. Probation will then send the cards to the State Department of Justice, which will conduct both DOJ and FBI background checks.

5.4.1.2. Driving record through the State of California Department of Motor Vehicle (DMV);

5.4.1.3. Drug testing.

5.4.1.4. Background check packages must be submitted to the Probation Department located at 9444 Balboa Avenue, Suite 500, San Diego, CA 92123 Attention: Background Division. The Contractor is advised to keep copies of all applications/background check packages submitted to the Probation Department.

5.4.1.5. Incomplete Packages will not be accepted. A typical background package includes:

5.4.1.6. A complete signed Security Clearance Request Form,

5.4.1.7. A clean, valid, and legible copy of Social Security Card or Social Security Administration abstract,

5.4.1.8. A clean, valid and legible copy of a Driver's license, or State-issued Identification Card,

5.4.1.9. For Contractor Employees who are not citizens of the United States: either a valid Resident Alien Badge or valid form of picture identification,

5.4.1.10. For Contractor Employees requesting electronic access authorization: a complete Access Registration Form

5.4.1.11. Contractors are required to submit one check covering the cost of the background check process for all employees. The check should be made payable to: County of San Diego. Questions regarding associated costs should be directed to the COR.

5.4.1.12. If applicable, Contractor must have completed Livescan applications for each Contractor Employee, agent, subcontractor, vendor and their employees in addition to the background package. Contractor shall obtain a Livescan application from the Probation Department. County may provide Contractor with information on various Livescan locations and fees. A fee is required by the Department of Justice and collected by the Livescan operator. Contractor shall pay all Livescan associated fees.

5.4.1.13. Background checks generally take 4-6 weeks to process. The Probation Department will notify Contractor directly, or through the COR, the results of submitted background checks. If the background screening results are acceptable, Contractor Employee may begin services under the Agreement.

5.4.1.14. Results of Criminal Background Clearance. If a background check indicates a criminal record inappropriate to be assigned to this Agreement, that individual shall not be assigned to perform services under the Agreement.

5.4.2. Inappropriate Criminal Record. An inappropriate criminal record may include, but is not limited to:

5.4.2.1. Felony convictions of any kind;

5.4.2.2. Convictions of crimes of moral turpitude (prostitution, sex offenses, etc.);

5.4.2.3. Exhibiting patterns of criminal behavior;

5.4.2.4. Exhibiting patterns of anti-social behavior;

5.4.2.5. Convictions for illegal immigrant smuggling;

5.4.2.6. Outstanding warrants and/or unresolved investigations;

5.4.2.7. A misdemeanor conviction;

5.4.2.8. More than three Failure to Appear citations within the last two years;

5.4.2.9. Receipt of subsequent arrest notices after approval and issuance of access to CORI/CLETS and/or a County facility, and/or

5.4.2.10. As otherwise required by federal and state law, including but not limited to Section 5.12 of the FBI Criminal Justice Information Services Security Policy and Section 1.9.2 of the California CLETS Policies, Practices and Procedures (PPP).

5.4.3. Review of Violations. County shall evaluate any Penal Code or other statutory violations individually and make a determination as to whether the violation precludes an individual's ability to efficiently carry out Agreement functions.

5.4.4. Removal of Employees, Volunteers or Subcontractors. Contractor shall immediately remove a Contractor Employee or agent, subcontractor or vendor from duties related to the Agreement if the updated clearance indicates a criminal record inappropriate to be assigned to the Agreement.

5.4.5. Duration of Background Checks. Background checks for Contract Employees and subcontractors, agents and vendors shall be valid for five years. Background reinvestigations shall be conducted every five years unless Rap Back is implemented. ("Rap Back" is a national fingerprint and criminal history system maintained by the FBI CJIS Division service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.)

5.4.6. Department of Motor Vehicles (DMV). Contractor shall obtain and review the DMV record of any of Contractor's Employees who are assigned to the Agreement and whose job duties include, or may include, driving. Such Contractor Employees are referred to in this section as "Drivers." Contractor shall enroll in the State of California's DMV Employer Pull Notice Program (EPN) and ensure that all staff are added and enrollment properly maintained. The EPN Program can be found at: Employer Pull Notice Program - California DMV.

5.4.6.1. Drivers shall have no more than three violation points for traffic violations, at fault accidents, and misdemeanor convictions within the last year. As stated in the Vehicle Code, Section 12810.5, "four or more points in 12 months…shall be prima facie presumed to be a negligent operator of a motor vehicle."

5.4.6.2. All Drivers shall maintain a valid California Driver License. Exceptions must be approved by the COR on a case-by-case basis prior to employment of contract staff.

5.4.7. Drug Testing. Contractor shall cause Contractor Employees assigned to the Agreement to undergo drug testing. No person shall be assigned to the Agreement who tests positive for any illegal drugs, including marijuana. Contractor shall also comply with County of San Diego Board of Supervisors Policy C-25, which can be found at: http://www.sdcounty.ca.gov/cob/policy/ .

5.4.7.1. Contractor shall subsequently conduct reasonable-suspicion testing of Contractor Employees as deemed necessary by Contractor.

5.4.8. Tuberculosis Testing. Contractor shall cause Contractor Employees assigned to the Agreement, and having direct contact with minors, to undergo annual testing for tuberculosis. Contractor may retest a Contractor Employee who tests positive for tuberculosis. Contractor may, in cases where a Contractor Employee has falsely tested positive in the past, accept a letter from the employee's physician that states that the employee is not exhibiting symptoms of active tuberculosis that would warrant additional x-rays and examination. Any Contractor Employee who is confirmed to have infectious tuberculosis shall not be assigned to Agreement functions where the Contractor Employee may come into contact with minors.

5.4.9. Contractor Employee, Agent, Subcontractor and Agent References. Contractor shall obtain and verify personal and prior employment references where available from Contractor Employees, subcontractors, agents and vendors assigned to the Agreement. Contractor shall evaluate any negative references and determine whether any such information precludes the employee from carrying out the functions of the Agreement.

5.4.10. Education Requirements. Contractor shall confirm compliance with education requirements as specified in the Agreement.

5.4.11. Exceptions. Exceptions to compliance with the aforementioned clearance requirements must be approved by the COR on a case-by-case basis.

5.4.12. Employee/Volunteer Statement. Per PPP section 1.5.1, all contractor employees, agents, volunteers and subcontract personnel with "physical and logical" access to CORI/CLETS shall sign the Employee/Volunteer Statement Form (Exhibit 12.1.1-3).

5.5. Maintenance of Records. Maintenance of CORI/CLETS Training Records: Parties shall maintain records of all training, testing, and proficiency affirmation of CORI/CLETS in accordance with section 1.8.3.A.3 of the PPP and shall be made available for inspection, upon request, by the other party.

5.6. Changes to Access. Contractor shall notify Probation of any changes in writing or email for Contractor Employees, agents, subcontractors or vendors assigned to the Agreement within thirty days of assignment or termination.

5.7. Private Management Control Agreement. In order to access the CLETS/CORI systems, the Contractor shall sign the Private Management Control Agreement (Exhibit 12.1.1-4).

5.8. Security Addendum. The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Addendum (Exhibit 12.1.1-5) shall be signed.

5.9. Compliance with Laws. All CORI/CLETS rules, regulations, policies, practices and procedures will be adhered to by all parties involved, at all times. Contractor's failure to comply with any applicable laws and regulations is considered a breach of security and may result in the termination for default of the Agreement.

6. PERSONNEL ACCESS

6.1. In addition to the other background requirements set forth in this Schedule 12.1.1, it is the "County's policy to require that all permanent, temporary and seasonal employees, contractors and volunteers be issued and display a County ID card while on duty and/or within County facilities". Therefore, Contractor personnel performing Services at a Location shall comply with (i) County Administration Manual 0040-06 County Identification / Access Card Program and (ii) Department of General Service Policy and Procedure – Facilities Section entitled 3.1.6 SECURITY, as described in Section 12.1.3 of the Agreement.

6.2. Background Investigation

6.2.1. Background Investigations

Background investigations on Contractor personnel shall be conducted in accordance with the Standards and Procedures Manual and the Department of General - Services Policy & Procedures sections entitled 3.1.6.1 SECURITY CARD ACCESS SYSTEM and 3.1.6.4 CONTRACT SERVICE PROVIDER SECURITY REQUIREMENTS.

All Contractor personnel requiring access to any IT and telecommunications system supporting the delivery of the Services shall have passed an employee background investigation that is equivalent to that of the County. If the Contractor's employee background investigation policy, processes and procedures does not meet County standards, then the Contractor may use the County's background investigation process to fulfill this requirement.

6.2.2. County's Notification to Contractor

Contractor will be notified in the event that any Contractor personnel do not pass the background investigation. The County will not provide reasons or comments justifying such decision. However, should Contractor believe that there has been a mistake, then Contractor may bring the matter to the attention of the CIO.

6.2.3. County Issued I.D. Cards

6.2.3.1. After each Contractor personnel has successfully passed background investigation, the County will issue a County identification card (County ID card). The County ID card identifies Contractor personnel as being authorized to enter County facilities for the performance of Services and must be worn at all times during the performance of Services within any of the County's facilities.

6.2.3.2. County I.D. cards are for the exclusive use of the individual named and pictured on the card. Such cards shall remain the property of the County and shall be returned upon demand, or upon the termination or resignation of the individual, or upon termination or expiration of the Agreement.

6.2.3.3. Contractor shall assume all responsibility for all Contractor personnel's use of and the return of the County I.D. cards. Contractor shall be assessed one hundred (100) dollars (or such other fee as may be set forth in the Standards and Procedures Manual) for each County I.D. card not returned to the County. At the expiration and or termination of the Agreement, all or a portion of final payment may, at County's sole discretion, be withheld until all cards are accounted for.

6.2.4. Keys for County Facilities

6.2.4.1. Contractor may be temporarily issued a set of keys for County facilities that do not have guards on duty. Contractor shall assume all responsibilities for the use and prompt return of the keys. Any Contractor personnel holding keys to the County facilities shall use such keys solely to gain access to perform Services.

6.2.4.2. Keys issued to Contractor shall remain the property of the County and shall be returned upon demand or upon the termination or expiration of the Agreement. In addition to any other costs or damages, Contractor shall be assessed one hundred (100) dollars (or such other fee as may be set forth in the Standards and Procedures Manual) for each key not returned and will be further assessed the actual cost for parts and locksmith services to remove the lost key from the facility keying system(s).

6.2.4.3. If any key or access control card (County I.D. card) is lost or stolen, Contractor shall immediately notify the CIO in writing with the following information: the facility for which key(s) was lost, who lost the key(s), where the key(s) was lost, and the date / time loss was discovered.

6.2.4.4. Unauthorized duplication of keys to County facilities is a misdemeanor under Chapter 3, Section 469 of the California, Standard Penal Code.

6.2.5. Alarm Systems

6.2.5.1. The County has alarm systems in numerous facilities. In some instances there are multiple alarm systems within a facility. Contractor may be issued alarm codes and be instructed to properly operate the alarm systems. Contractor shall ensure that any Contractor personnel operating the alarm system be fluent in English. Failure to operate the alarm system correctly will result in a false alarm. Contractor will be responsible for all costs associated with false alarms.

6.2.5.2. In the event of a life threatening emergency, Contractor will instruct its personnel to use the standard operating procedures for emergency response, i.e. to call 911.

7. MISCELLANEOUS

7.1. Disclaimer. County makes no guarantee that compliance with this Agreement will be satisfactory for the Contractor's own purposes.

7.2. Amendment. The Parties agree to take action as necessary to amend this Schedule 12.1.1 from time-to-time as is necessary for County to comply with the requirements of any and all applicable other federal or State laws and regulations.

7.3. Judicial or Admin Proceedings. Contractor will notify County if it is named as a defendant in any criminal, civil, or administrative proceeding for a violation of any applicable security or privacy law.

7.4. Assistance in Litigation or Admin Proceedings. Contractor shall make itself and any of its agents available, at no cost to County, to testify, or otherwise, in the event of litigation or administrative proceedings commenced against County, its directors, officers, or employees, based on claimed violations of any applicable confidentiality, privacy, or security law or regulation, whether federal or State, if that litigation or proceeding involves actions of Contractor or its agents, except those where Contractor or its agents are named as an adverse party.

7.5. Interpretation. Any ambiguity in this Schedule 12.1.1 shall be resolved in favor of a meaning that permits County to comply with the applicable federal or State law or regulation.

7.6. Conflict. If a conflict between any of the standards contained in any of these enumerated sources of standards is found, Contractor shall follow the most stringent standard. The most stringent standard means that safeguard which provides the highest level of protection to County PHI and/or County PII/PI from unauthorized disclosure.

7.7. Regulatory References. All references in this Schedule 12.1.1 to any regulation or law mean the regulation or law currently in effect, including those legal and regulatory changes that occur after the effective date of this Agreement.

7.8. Survival. The respective rights and obligations of County and Contractor under this Schedule 12.1.1 shall survive the termination of the Agreement.

7.9. No Waiver of Obligations. No change, waiver, or discharge of any liability or obligation hereunder or any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, an any other occasion.

7.10. Due Diligence. Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Schedule 12.1.1 and is in compliance with all applicable federal and State laws and regulations, and that its agents, subcontractors, and vendors are in compliance with their obligations as required by this Schedule 12.1.1.

7.11. Effect of Termination. Upon termination of the Contract, for any reason, with respect to any and all County PHI and/or County PII/PI received from County, or created or received by Contractor on behalf of County:

7.11.1. Contractor shall return or destroy all County PHI and/or County PII/PI and retain no copies of County PHI and/or County PII/PI, except County PHI and/or County PII/PI necessary for Contractor to continue its proper management and administration or to carry out its legal responsibilities, as mutually agreed upon by the Parties.

7.11.2. Upon mutual agreement of the Parties that return or destruction of County PHI and/or County PII/PI is infeasible, Contractor shall extend the protections of this Schedule to such County PHI and/or County PII/PI for so long as Contractor maintains such County PHI and/or County PII/PI.

7.11.3. Contractor shall return to County or destroy, as determined by County, County PHI and/or County PII/PI retained by Contractor when it is no longer needed by Contractor for its proper management and administration or to carry out its legal responsibilities.

7.11.4. This provision shall apply to County PHI and/or County PII/PI that is in the possession of subcontractors or agents of Contractor.

END OF SCHEDULE

Exhibit 12.1.1-1 – County Privacy Incident Report Form

Privacy Incident Report

STAFF INVOLVED (IF APPLICABLE)

Contractor Name:
Name of COR: **COR Phone Number:**

Name/s of Staff Involved in Incident:

Date of Staff/s Last Privacy Training:

Job Title/s and Primary Job Duties of Staff Involved:

INCIDENT DETAILS

Describe Incident (include location of incident, how it occurred, type of media, and details regarding type of Protected Information involved):

DO NOT INCLUDE ANY PROTECTED INFORMATION ON THIS REPORT

Date Incident Occurred:

Was Police Report Filed? ☐ Yes ☐ No ***If yes**, Report #:*

If report is being made more than 1 day after the incident, explain delay:

Was staff in violation of any County Contract requirement and/or Contractor Policy? ☐ Yes ☐ No
If yes, which policy or requirement?

DATA INVOLVED

Number of Individuals' Data Involved:
(If number of individuals is an estimate, check here ☐)

Provide a breakdown of the individuals whose data was involved.
Specify # individuals on public benefits (ie Medi-Cal), what type of public benefits, and whether a minor or adult, if known:

Type/s of Media Involved: *Check all that apply:*
☐ Paper ☐ Email ☐ Flash Drive
☐ Smart Phone ☐ Cell Phone (not a Smart Phone)
☐ Desktop ☐ Laptop ☐ Tablet *If County device, Asset #*:
☐ Computer System; system name:
☐ Other media; explain:

Types of Electronic Files Involved: *Check all that apply*
☐ MS Word file ☐ MS Excel or CSV File ☐ Adobe (.PDF)
☐ Computer System (such as Anasazi or CalWIN) Print Outs or Screen Shots; Name of System:
☐ Other; explain:

Type of Data Involved: *Check all that apply.*
☐ First Name or Initial ☐ Last Name
☐ CIN or Medi-Cal # ☐ SSN
☐ Address/Zip Code ☐ Phone/Fax
☐ Case number ☐ Driver's License
☐ DOB ☐ Other Dates tied to Case
☐ Membership # ☐ Any other number
☐ User Name/Email Address & Password
☐ Health Plan Name (including Medi-Cal)
☐ Credit Card/Bank Acct# ☐ Diagnosis
☐ Drug/Alcohol Tx Info ☐ HIV/AIDS Info
☐ Mental Health Info ☐ Lab Results
☐ Health or medical information
☐ Psychotherapy Notes
☐ Other Case Info (including benefits status)
☐ Appointment Info ☐ EBT Number
☐ Other; explain:

MITIGATIONS

Describe Data Security (such as locks, encryption):

Encryption: Was data encrypted per NIST standards? ☐ Yes ☐ No

If incident involves laptop, tablet, or phone: Was it wiped after discovery? Date wiped**:**
If device was not wiped, explain why:

Was data eventually recovered? ☐ Yes Explain how, when, and who now has data:

☐ No Explain why not recovered and attempts to retrieve:

If incident involves email, date confirmation received that email was permanently deleted by recipients:

Describe Corrective Action Plan and completion date (or estimated date):

Do you have reason to believe data was viewed by an unauthorized person?: ☐ Yes ☐ No **Explain:**

SIGNATURE

Signature Of Staff Completing Form:

Date:

Name of Staff Completing Report (Staff completing form cannot be involved in incident):

Title:

Phone #:

Exhibit 12.1.1-2 – CORI-CLETS Training Request Form

COUNTY CONTRACT NUMBER 554833
EXHIBIT 12.1.1-2

Criminal Offender Record Information (CORI) Training Requirement:

Penal Code Section 11075 and 11077(d) requires the County to ensure that only a certified CLETS/NCIC trainer initially trains all sworn/non-sworn, non-criminal justice, **volunteer and contractor personnel**, with "physical and logical access" to CLETS, NCIC and CORI within six months of assignment. CORI training has to be scheduled within 30 days of assignment.

Contract Staff Information:

Request to Enroll the Following Staff in CORI Training: ☐ Contract ☐ VIP ☐ Other: _____

First and Last Name (Print): _____

Staff E-mail Address (Print): _____

Program Name: _____

Date Assigned to Program: _____

Work Address: _____

Contractor or VIP Group: _____

If Contract Staff is Replacing Someone, Print First & Last Name: _____

Contract Supervisor First and Last Name _____

Contract Supervisor Signature: x _____ Date: _____

Contract Supervisor E-mail Address _____

County (non-Probation) COTR/Designee: COTR/Designee First and Last Name: _____

County (non-Probation) COTR/Designee Signature: x _____ Date: _____

Probation COTR/Designee:

Type of CORI Training: ☐ 1½ Hour ☐ 4 Hour

Contract Analyst First and Last Name (Print): _____

COTR/Designee First and Last Name (Print): _____

COTR/Designee Signature: x _____ Date: _____

Contractor: *Please forward to COTR/County Designee or Probation COTR/Designee.*

COTR/County Designee: *Please forward to Probation COTR/Designee.*

Probation COTR/Designee: *Please forward to Probation Contract Analyst (e-mail, or fax to: 858.514.3222).*

Contract Analyst: *Please forward to Staff Development for scheduling (Probation.StaffDevelopment@sdcounty.ca.gov).*

Staff Development: *Please send the scheduled training date and time to the Probation COTR/Designee and Contract Analysis*

END OF SCHEDULE

Exhibit 12.1.1-3 – Employee-Volunteer Statement Form

CLETS EMPLOYEE/VOLUNTEER STATEMENT

Print Form

Use of information from the California Law Enforcement Telecommunications System (CLETS) and the Department of Motor Vehicles record information

As an employee/volunteer of San Diego County Probation Department, you may have access to confidential criminal records, the Department of Motor Vehicle records or other criminal justice information, much of which is controlled by statute. All information from the CLETS is based on the "need-to-know" and the "right-to-know" basis. The misuse of such information may adversely affect an individual's civil rights and violates the law and/or CLETS policies.

Penal Code (PC) section 502 prescribes the penalties relating to computer crimes. PC sections 11105 and 13300 identify who has access to state and local summary criminal history information and under which circumstances it may be released. PC sections 11141-11143 and 13302-13304 prescribe penalties for misuse of state and local summary criminal history information. Government Code section 6200 prescribes the felony penalties for misuse of public records and information from the CLETS. California Vehicle Code section 1808.45 prescribes the penalties relating to misuse of the Department of Motor Vehicle record information.

Penal Code sections 11142 and 13303 state:

> **"Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."**

Any employee/volunteer who is responsible for the CLETS misuse is subject to immediate dismissal from employment. Violations of the law may result in criminal and/or civil action.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL INFORMATION FROM THE CLETS.

Signature

Print Name

Date

Exhibit 12.1.1-4 – Private Management Control Agreement

CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

Print Form

Agreement to allow California Law Enforcement Telecommunications System (CLETS) access by

_____ (Public law enforcement/criminal justice agency) , _____ (ORI)

to _____ (Private Contractor)

to perform _____ (Type of service) services on its behalf.

Access to the CLETS is authorized to public law enforcement and criminal justice agencies (*hereinafter referred to as the CLETS subscribing agency*) only, which may delegate the responsibility of performing the administration of criminal justice functions (e.g., dispatching functions or data processing/information services) in accordance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Addendum to a private contractor. The private contractor may access systems or networks that access the CLETS on behalf of the CLETS subscribing agency to accomplish the above-specified service(s). This agreement must be received by the California Department of Justice (CA DOJ) prior to the subscribing agency permitting access to the CLETS. The performance of such delegated services does not convert that agency into a public criminal justice agency, not automatically authorize access to state summary criminal history information. Information from the CLETS is confidential and may be used only for the purpose(s) for which it is authorized. Violation of confidentiality requirements or access authorizations may be subject to disciplinary action or criminal charges.

Pursuant to the policies outlined in the *CLETS Policies, Practices, and Procedures (PPP)* and the Federal Bureau of Investigation's (FBI) *CJIS Security Policy*, it is agreed the CLETS subscribing agency will maintain responsibility for security control as it relates to the CLETS access. Security control is defined as the ability of the CLETS subscribing agency to set, maintain, and enforce:

1. Standards for the selection, supervision, and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant CLETS access to personnel who meet these standards and deny it to those who do not.

2. Policies governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support a telecommunications network and related CA DOJ criminal justice databases used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Security control includes, but is not limited to, the supervision of applicable equipment, systems design, programming, and operating procedures associated with the development, implementation, and operation of any computerized message-switching or database systems utilized by the served law enforcement agency or agencies. Computer sites must have adequate physical security to protect against any unauthorized viewing or access to computer terminal, access devices, or stored/printed data.

CLETS PRIVATE CONTRACTOR MANAGEMENT CONTROL AGREEMENT

Additionally, it is the responsibility of the CLETS subscribing agency to ensure that all private contractors receiving information from the CLETS meet the minimum training, certification, and background requirements that are also imposed on the CLETS subscribing agency's staff. The minimum requirements are applicable also to staff having access to record storage areas containing information from the CLETS. The minimum requirements include, but are not limited to:

1. Prior to allowing the CLETS access, train, functionally test, and affirm the proficiency of all the CLETS computer operators to ensure compliance with the CLETS and the FBI's National Crime Information Center (NCIC) policies and regulations, if applicable. Biennially, provide testing and reaffirm the proficiency of all the CLETS operators, if applicable.

2. State and FBI criminal offender record information searches must be conducted prior to allowing access to the CLETS computers, equipment, or information. If the results of the criminal offender record information search reveal a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted.

3. Each individual must sign a CLETS Employee/Volunteer Statement form (HDC 0009) prior to operating or having access to CLETS computers, equipment, or information.

In accordance with CLETS/NCIC policies, the CLETS subscribing agency has the responsibility and authority to monitor, audit, and enforce the implementation of this agreement by the private contractor. The private contractor agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement and to accomplish the directives for service under the provisions of this agreement. The CLETS Management Control Agreement (HDC 0004B) shall be updated when the head of either agency changes or immediately upon request from the CA DOJ.

By signing this agreement, the vendors and private contractors certify they have read and are familiar with the contents of (1) the FBI's CJIS Security Addendum, (2) the NCIC 2000 Operating Manual, (3) the FBI's CJIS Security Policy, (4) Title 28, Code of Federal Regulations, Part 20, and (5) the CLETS PPP and agree to be bound by their provisions. Criminal offender record information and related data, by its very nature, is sensitive and has potential for great harm if misused. Access to criminal offender record information and related data is therefore limited to the purpose(s) for which the CLETS subscribing agency has entered into the contract. Misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; use, dissemination, or secondary dissemination of information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. Accessing the system for an appropriate purpose and then using, disseminating, or secondary dissemination of information received for another purpose other than execution of the contract also constitutes misuse. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Signature (CLETS Subscribing Agency Head)	Signature (Private Contractor Agency Head)
Print Name and Title	Print Name and Title
Date	Date

Exhibit 12.1.1-5 – Federal Bureau of Investigations Criminal Justice Information Services Security Addendum

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Print Form

CERTIFICATION

I hereby certify that I have read and am familiar with the contents of (1) the Security Addendum, (2) the NCIC 2000 Operating Manual, (3) the Policy and Reference Manual, (4) the CJIS Security Policy, and (5) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal offender record information and related data is therefore limited to the purpose(s) for which a government agency entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things, accessing it without authorization, accessing it by exceeding authorization, accessing it for an improper purpose, using, disseminating, or re-disseminating information received for another purpose other than the execution of the contract also constitutes misuse. I further understand the occurrence of misuse does not depend upon whether I receive additional compensation for such authorized activity. Such exposure for misuse include, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Signature of Contractor Employee _____ Date _____

Signature of Contractor Representative _____ Date _____

Organization and Title _____

Schedule 14.1 – Approved Subcontractors

Table of Contents

1. Overview 3

2. Key Subcontractors of Contractor 3

1. OVERVIEW

Contractor shall provide listing of all Key Subcontractors as defined in Terms and Conditions, Section 14 – Use of Affiliates and Subcontractors, in this Schedule 14.1.

2. KEY SUBCONTRACTORS OF CONTRACTOR

Name	Date Added to Schedule
AT&T Enterprises, LLC	CED
Adecco	CED
TEKSystems	March 28, 2019
DXC	April 3, 2019
IBM	April 29, 2019

END OF SCHEDULE

Schedule 16.1 – Fees

Table of Contents

1. OVERVIEW 4

2. EXHIBITS AND APPENDICES 4

3. TRANSITION SERVICES 4

4. DEFINED TERMS 5
4.1. Banding 5
4.2. Baseline Volume 5
4.3. Bundled Resource Unit 5
4.4. Resource Unit Fee 5

5. DISENTANGLEMENT FEES 6

6. CAPITALIZATION AND DEPRECIATION 6
6.1. Capitalization 6
6.2. Depreciation 7

7. RESOURCE UNIT FEES 7
7.1. Monthly Service Charge 7
7.2. Volumes Outside of Existing Bands 8
7.3. Addition and Removal of Resource Units 9
7.4. Addition and Removal of Resource Unit Volumes 9

8. CROSS FUNCTIONAL SERVICES 9
8.1. Contract and Acquisition Management Services 9
8.2. Domain Name Management Services 12
8.3. Business Analyst Services 12
8.4. Chief Technical Architect Services 12
8.5. Enterprise Application Architect Services 12
8.6. Innovation Management Services 13
8.7. Project Management Services 14

9. SERVICE DESK SERVICES 14

10. END USER SERVICES 14
10.1. Early Refresh 14
10.2. [reserved] 15
10.3. Catalog Services 15
10.4. Electronic Signature Services 17
10.5. Digital Signage Services 17
10.6. Survey Solution Support Services 17
10.7. Electronic File Sharing Services 18

11. NETWORK SERVICES 18
11.1. Voice Services 18
11.2. Network Access 20
11.3. Remote Site Redundancy for Key County Sites 21
11.4. Remote Site Redundancy for T-1 Site 21
11.5. New Site Installation Services 21
11.6. Zoom Video Support Conferencing Services 23
11.7. Mobility Services 24

12. DATA CENTER SERVICES 25
12.1. Infrastructure Services 25
12.2. Development and Test Services 25
12.3. Storage and Data Management Services 25
12.4. Cloud Services 26
12.5. Low Code Application Platform – Outsystems 27

13. APPLICATIONS SERVICES 27
13.1. Application Maintenance and Operations Services 27
13.2. Application Development Services 28

14. SPECIAL SERVICE LEVELS 29
14.1. Registrar of Voters 29
14.2. Treasurer-Tax Collector 30
14.3. Assessor / Record / County Clerk (ARCC) Acclaim 30

1. OVERVIEW

Exhibit 16.1 – Fees, including the Exhibits and Appendices attached hereto, describes the methodology for billing with respect to the Services provided under the Agreement. The Fees set forth herein represent the total amounts payable by the County with respect to all Services to be performed under the Agreement, whether or not a particular Service is associated with a particular Resource Unit Fee. All capitalized terms used and not defined in this Schedule shall have the meanings given to them in Schedule A – Definitions. All references to Exhibit 16.1-1 below shall be deemed to be references to Exhibit 16.1-6 for purposes of calculating applicable fees and credits during the Option Term.

2. EXHIBITS AND APPENDICES

The Exhibits and Appendices set forth in the table of contents above are attached to this Schedule 16.1 and incorporated hereto.

Reference Number	Title
Exhibit 16.1-1	Resource Unit Summary
Exhibit 16.1-1a	Fees Sample Calculations
Exhibit 16.1-1 Appendix 1	New Site Install Variable Components
Exhibit 16.1-2	Resource Unit Price Decomposition
Exhibit 16.1-3	Maximum Annual Fee
Exhibit 16.1-4	Labor Categories
Exhibit 16.1-5	Firm Fixed Price for Applications Maintenance and Operations
Exhibit 16.1-5b	Firm Fixed Price for Applications Maintenance and Operations
Exhibit 16.1-6	Resource Unit Summary Option Term
Exhibit 16.1-7	ELA Pricing Adjustments

3. TRANSITION SERVICES

Contractor shall perform all Services with respect to Transition on a milestone payment basis as further set forth below.

Transition Milestone	Milestone Date	Transition Fees
Cutover of the Service Desk Services Framework	4/30/2018	$0.00
Cutover of the Application Services Framework	6/30/2017	$0.00

Transition Milestone	Milestone Date	Transition Fees
Cutover of the End-User Services Framework	7/31/2017	$0.00
Cutover of the Network Services Framework	8/31/2017	$0.00
Cutover of the Data Center Services Framework	4/30/2018	$0.00
Cutover of the Cross Functional Services	4/30/2018	$0.00
Full and complete transition of all Service Frameworks	4/30/2018	$ 7,212,700.17

The Milestone Date refers to the date by which the applicable Transition Milestone must be achieved. The Transition Fees refers to the Fee associated with completion and acceptance by the County of Transition Milestone. In the event that Contractor fails to meet a Transition Milestone by the Milestone Date set forth above, the County may decrement any amount of Transition Fees applicable to such Critical Milestone reasonably determined by the County to represent the diminishment in value of the Services to the County and not as a penalty.

4. DEFINED TERMS

4.1. Banding

"Banding" shall mean incremental decrease or increase in Resource Unit Fees due to the volume of Resource Units consumed above or below the defined Baseline Volume.

4.2. Baseline Volume

"Baseline Volume" shall mean, for any Resource Unit, the specified quantities of such Resource Units as set forth in Exhibit 16.1-1.

4.3. Bundled Resource Unit

"Bundled Resource Units" shall mean Resource Units indicated on Exhibit 16.1-1 for which the Baseline Volumes and the County's actual volumes of consumption are each aggregated for the purposes of determining in which Resource Unit Fee band the individual Resource Units in such bundle are to be charged.

4.4. Resource Unit Fee

"Resource Unit Fee" shall mean, for any Resource Unit, the specified charge for such Resource Unit as set forth in Exhibit 16.1-1.

5. DISENTANGLEMENT FEES

For any termination as set forth in Section 17 of the Agreement and during the period of any Disentanglement of any Terminated Services, the County shall only pay the Resource Unit Fee for the 90% to 110% range for such Resource Unit.

6. CAPITALIZATION AND DEPRECIATION

Except for Shared Resources, all such acquisitions shall, for purposes of the County's rights upon Disentanglement pursuant to Section 6.3.6 of the Agreement be capitalized, accounted for, and depreciated by Contractor in accordance with the guidelines set forth in herein, without regard to the actual method of acquisition (i.e., whether by purchase, lease, or other method of financing).

6.1. Capitalization

Assets used to provide the Services shall be capitalized as follows:

6.1.1. Computing Hardware

Computing hardware shall be capitalized and depreciated if the cost is $5,000 or greater and the useful life is greater than one (1) year. Computer workstation components required to make the workstation functional, are typically grouped as a system to determine the capitalization threshold. Capitalized amounts include equipment cost, sales tax, shipping, and installation.

6.1.2. Computing Software

Computer software shall be capitalized and depreciated per the following:

6.1.2.1 COTS – if the cost is $50,000 or greater and the useful life is greater than one (1) year.

6.1.2.2 Internally Developed – if the cost is $100,000 or greater and the useful life is greater than one (1) year.

6.1.2.3 Operating system Software that is required to make a system functional is capitalized as part of the system.

6.1.2.4 Capitalized PC and server Software is depreciated over the life of the hardware asset.

Capitalized amounts include Software cost, sales tax, shipping, and installation.

6.1.3. Software Agreements

Software agreements shall be capitalized and depreciated if the cost is $50,000 or greater and the useful life is greater than one (1) year. Multiyear license agreements must be at least $50,000 for each year of the agreement.

6.1.4. Voicemail and Network Infrastructure

Hardware and software for voice and network are capitalized and depreciated if the cost is $5,000 or greater and the useful life is greater than one (1) year. Capitalized amounts include equipment cost, sales tax, shipping and installation.

6.1.5. Leasehold Improvements

Leasehold Improvements are capitalized if the project is $25,000 or more and depreciated over the shorter of the estimated useful life of the improvement or the life of the lease.

6.1.6. Furniture

Free standing furniture and fixtures are capitalized if the cost is $5,000 or greater and the useful life is a minimum of two (2) years. The assets must also be identifiable and controllable.

6.2. Depreciation

Assets used to provide the Services applicable to a Resource Unit shall be depreciated using the straight line method over the number of years indicated in Exhibit 16.1-1 for such Resource Unit.

7. RESOURCE UNIT FEES

This section pertains to the methodology of Resource Unit Fee calculations and changes related to Resource Unit Fee and/or its volumes.

7.1. Monthly Service Charge

Following Cutover for each Service Framework during the Term, Contractor shall calculate, on the last day of each calendar month on either a snapshot or cumulative basis as indicated in Exhibit 16.1-1, the quantity of Resource Units applicable to such Service Framework utilized by the County during that month. Contractor shall report such quantities to the County in accordance with the format described in Section 16.2 and Schedule 5 of the Agreement, together with the supporting

information and documentation required under such Section and Schedule. Such quantities shall be used to calculate the Monthly Services Charge as follows:

7.1.1. Non-Bundled Resource Units

The County's actual monthly volume for Non-Bundled Resource Units shall be multiplied by the applicable Resource Unit Fees as set forth in Exhibit 16.1-1 and, if applicable, corresponding to the volume band in which the County's actual volume of consumption falls during such month. An example of this calculation is set forth in Appendix 16.1-1a.

7.1.2. Bundled Resource Units

If the County's actual monthly volume for Bundled Resource Units falls between 90% and 110%, inclusive, of the sum of the Baseline Volumes for such Bundled Resource Units, then the actual monthly volume of each Resource Units in such bundle shall be multiplied by the applicable Resource Units Fee for the 90% to 110% range as set forth in Exhibit 16.1-1, even if the actual monthly volume for a particular Resource Unit falls outside of such range.

If the County's actual monthly volume for Bundled Resource Units outside the 90% to 110% range described above, then the actual monthly volume of each Resource Unit in such bundle shall be multiplied by the applicable Resource Unit Fee as set forth in Exhibit 16.1-1 corresponding to the volume band in which the County's actual volume of consumption of such individual Resource Unit falls during such month. An example of this calculation is set forth in Appendix 16.1-1a.

7.2. Volumes Outside of Existing Bands

7.2.1. Non-Bundled Resource Units

If, in any Contract Year, the County's actual consumption is (i) greater than one hundred thirty percent (130%) of the Baseline Volume for such Resource Unit or (ii) is less than seventy percent (70%) of the Baseline Volume for such Resource Unit, then the Parties shall negotiate in good faith new pricing bands, as applicable, for such Resource Units. While such negotiations are pending, the County's consumption of such Resource Units shall continue to be invoiced at the then current Resource Unit Fees for such Resource Units until the Parties establish new pricing bands for such Resource Units.

7.2.2. Bundled Resource Units

If, in any Contract Year, the County's actual consumption is (i) greater than one hundred thirty percent (130%) of the sum of the Baseline Volumes for the Resource Units in the same group of Bundled Resource Units as indicated in Exhibit 16.1-1 or (ii) is less than seventy percent (70%) of the sum of the Baseline Volumes for the Resource Units in the same group of Bundled Resource Units as indicated in Exhibit 16.1-1, then the Parties shall negotiate in good faith new pricing bands, as applicable, for such Resource Units. While such negotiations are pending, the County's consumption of such Resource Units shall continue to be invoiced at the then current Resource Unit Fees for such Resource Units until the Parties establish new pricing bands for such Resource Units.

7.3. Addition and Removal of Resource Units

The Parties may add or remove Resource Units upon mutual written agreement. For the purposes of added Resource Units, Contractor may charge the County for such Resource Unit commencing on the date the Contractor obtains a signature from an authorized representative of the County confirming the County's acceptance of the delivery and/or installation of such Resource Unit. For the purposes of removed Resource Units, Contractor shall no longer charge the County for and the County shall have no obligation to pay for such Resource Units as of, and after the date that the County submits a request for the removal of such Resource Units that is executed by an authorized representative of the County.

7.4. Addition and Removal of Resource Unit Volumes

Resource Units may only be added to or removed from the County's volumes pursuant to a written acceptance of the addition or removal of a Resource Unit executed by an authorized representative of the County.

8. CROSS FUNCTIONAL SERVICES

This section pertains to the Fees associated with Section 2 – Cross Functional Services in Schedule 4.3 and listed in Exhibit 16.1-1.

8.1. Contract and Acquisition Management Services

8.1.1. Third Party Agreements

As part of the Services, Contractor will administer for the County certain Hardware and Software that is in addition to the Hardware and Software that Contractor uses to provide the Services described in the Schedules and for which Contractor is paid a Resource Unit Fee or other Fee. Contractor's administration responsibilities for this Hardware and Software

include, as set forth below, procurement (market analysis, competitive or sole source procurement, negotiation of agreements, licenses, amendments, and the like), administration of license, maintenance and service agreements, Service Desk support, payment, tracking of the Hardware and Software (including the license and service provisions, limitations, expiration and renewal periods), maintenance agreements (including agreement provisions, limitations, expiration and renewal periods), and tracking and reporting on the status of the administration of the Hardware and Software on the Service Portal described in Schedule 4.3, Cross Functional Section 2.3, and any other administrative or management related activities.

The Resource Unit approach to Third-Party Agreements is set forth in the table below and examples of calculation are set forth in Appendix 16.1-1a.

Resource	Description	Fee
Third Party Negotiation – Large	Negotiation of an agreement with a new Third-Party vendor in excess of $500,000.	$10,000
Third Party Negotiation – Small	Negotiation of an agreement with a new Third-Party vendor up to $500,000.	$5,000

<table>
<tr><th>Resource</th><th>Description</th><th>Fee</th></tr>
<tr><td>Third Party Transaction</td><td>Fees applied to a Transaction for products and/or services which are not provided by services for which Contractor is paid a Resource Unit.

Transaction is defined as a master contract with a Third-Party in which multiple Purchase Orders (POs) and PO Change Requests may be submitted to Third-Party. If there is no master contract with a Third-Party, Transaction is defined as a PO and PO Change Request(s) submitted to Third-Party.

• Fee percentages are calculated based on the Transaction amount and applied to the invoice amount. In the event of a multi-year license agreement, Fees are calculated on the aggregate charges. In addition, if a true up is required, the applicable fee shall be calculated on the true up amount.</td><td>1. For the following products and services, the Fee is 5% of the Transaction amount with a minimum fee of $100 and maximum fee of $50,000:
• Portfolio Software - Perpetual License Purchase
• Portfolio Software - Perpetual License Maintenance Renewal
• Hardware
• Hardware Maintenance
• Universal Power Supply (UPS)

2. For the following products and services, there is a tiered Fee structure per table below based on the Transaction amount:
• Labor Statement of Work
• Labor Agency Contractor
• Portfolio Software - SaaS
• Portfolio Software - Subscription

<table><tr><th>Percentage Tier</th><th>Transaction Amount</th></tr><tr><td>5%</td><td>Up to $1M</td></tr><tr><td>4%</td><td>Greater than $1M – up to $10M</td></tr><tr><td>3%</td><td>Greater than $10M</td></tr></table>
When a Change Request modifies a Transaction such that a different percentage tier applies, the applicable tier will be applied when the transaction amount threshold is reached.</td></tr>
</table>

A new third-party vendor is defined as a vendor with whom Contractor does not have a current agreement applicable to the transaction, whether never existed or expired, for which new terms and conditions must be negotiated. In the event that Third-Party Negotiation RUs apply, Contractor will notify the County in advance.

8.1.2. Pre-Approved Vendors List

Contractor shall maintain a minimum number of pre-approved vendors based on County demand:

Contract Year	Number of Procurement Requests	Minimum Pre-Approved Vendors
CY1	n/a	Five (5)
CY2 – CY7	< 15	Five (5)
	15 – 25	Seven (7)
	26 – 50	Ten (10)
	51+	Fifteen (15)

8.2. Domain Name Management Services

As part of the Domain Name Management Services, Contractor shall administer and manage all domain names for the County to meet the requirements described in Schedule 4.3, Cross Functional section 2.20. County will be charged a fixed monthly Resource Unit Fee for this service, as listed on Exhibit 16.1-1, for an unlimited number of domain names. The fixed monthly Resource Unit Fee includes transfer of County managed domain names to Contractor.

8.3. Business Analyst Services

As part of the Business Analyst Services, Contractor shall provide the County with five (5) Full Time Equivalent (FTE) Business Analyst positions to meet the requirements described in Schedule 4.3, Cross Functional section 2.21. The pool of 5 FTEs is subject to resource management at County discretion. County will be charged a fixed monthly Resource Unit Fee for this service, as listed on Exhibit 16.1-1. The Business Analyst Resource Unit Fee, which is an hourly labor rate, shall only apply if County requests an additional Business Analyst(s) for work not covered by the 5 FTEs provided in the Business Analyst Services.

8.4. Chief Technical Architect Services

As part of the Chief Technical Architect Services, Contractor shall provide the County with one (1) Full Time Equivalent Chief Technical Architect position to meet the requirements described in Schedule 4.3, Cross Functional section 2.22, Exhibit 16.1-4, and Schedule 10.1.1. County will be charged a fixed monthly Resource Unit Fee for this service, as listed on Exhibit 16.1-1.

8.5. Enterprise Application Architect Services

As part of the Enterprise Application Architect Services, Contractor shall provide the County with one (1) Full Time Equivalent Enterprise Application Architect position to meet the requirements described in Schedule 4.3, Cross Functional section 2.23, Exhibit 16.1-4, and Schedule 10.1.1. County will be charged a fixed monthly Resource Unit Fee for this service, as listed on Exhibit 16.1-1. Other architect services (e.g., applications architect) will be charged using the Resource Units in Exhibit 16.1-1 based on Labor Categories in Exhibit 16.1-4.

8.6. Innovation Management Services

8.6.1. Overview

As part of the Innovation Management Services, Contractor shall provide the County with one (1) Full Time Equivalent Innovation Officer (IO) position to meet the requirements described in Schedule 4.3, Cross Functional section 2.24, Exhibit 16.1-4, and Schedule 10.1.1. County will be charged a fixed monthly Resource Unit (RU) Fee for this service, as listed on Exhibit 16.1-1.

In Year 1 of the Agreement, the IO will be deployed for this Service. Effective Year 2 of the Agreement, the IO can be supplemented by additional staff based on the recommendation of the IO and approval of the CIO.

8.6.2. Innovation Fund

County and Contractor shall establish the Innovation Fund to support the Innovation Management Services activities. The parties will manage the Innovation Fund jointly.

8.6.3. Funding

The County and Contractor will co-fund the Innovation Fund. Effective Year 2 of the Agreement, both parties will contribute $500,000 on an annual basis thereby making available $1,000,000 in the Innovation Fund per year for innovation-related activities. The parties may change the funding by written agreement.

8.6.4. Use of Innovation Fund

Innovation Fund shall be used to add staffing to the Core Innovation Team on as needed basis, as mutually agreed to by the Contractor and County. The parties shall use either the Core Innovation Team Member Resource Unit or applicable Labor Category Resource Unit, whichever rate is lowest. Innovation Fund may also be used for rapid-cycle experiments, fast-

fail and agile proofs of concepts, Infrastructure as a Service (IaaS) cloud environments (e.g., AWS) to support Innovation activities, subject matter expert support to augment Innovation activities and material costs to perform Innovation activities approved by a joint governance committee consisting of County and Contractor personnel.

The County and Contractor will split all innovation projects costs 50/50 and, as much as possible, Contractor will leverage the Resource Units in the existing Agreement as the basis for pricing. Should the parties jointly agree to go outside of the Innovation Fund for costs incurred, the County will be charged 50% of the applicable Resource Unit Fee.

8.7. Project Management Services

As part of the Project Management Services, Contractor shall administer and manage a Project Management Office (PMO) to meet the requirements described in Schedule 4.3, Cross Functional section 2.9. County will be charged a fixed monthly Resource Unit Fee for this service, as listed on Exhibit 16.1-1. Project management for Applications Development-related activities will be charged according to the Labor Categories and associated Resource Units in Exhibits 16.1-4 and 16.1-1, respectively. Project management for infrastructure-related activities is covered within the Resource Units and will not be charged separately.

9. SERVICE DESK SERVICES

Reserved.

10. END USER SERVICES

This section pertains to the Fees associated with Section 4 – End User Services in Schedule 4.3 and listed in Exhibit 16.1-1.

10.1. Early Refresh

This section pertains to the Fees associated with Section 4.5.4 – Early Refresh in Schedule 4.3 and listed in Exhibit 16.1-1.

10.1.1. Early Refresh – Desktop

The Early Refresh – Desktop Resource Unit Fee shall apply if County requests to replace a desktop asset with more than six (6) months remaining prior to schedule refresh date and the replacement asset is of a different technology (e.g. Desktop - Engineering

Workstation to Laptop). An upgrade to the newest version of an asset is ineligible for Early Refresh. County will be charged the Resource Unit Fee listed in Exhibit 16.1-1 for each remaining month until the schedule refresh date.

10.1.2. Early Refresh – Mobile PC

The Early Refresh – Mobile PCs Resource Unit Fee shall apply if County requests to replace a Mobile PC asset with more than six (6) months remaining prior to schedule refresh date and the replacement asset is of a different technology (e.g. Laptop – Standard to Tablet - Convertible). An upgrade to the newest version of an asset is ineligible for Early Refresh. County will be charged the Resource Unit Fee listed in Exhibit 16.1-1 for each remaining month until the schedule refresh date.

10.2. [reserved]

10.3. Catalog Services

This section pertains to the Fees associated with Section 4.10 – Catalog Services in Schedule 4.3.

10.3.1. Optional Item Catalog

As described in Schedule 4.3, the Contractor shall provide and maintain an online Optional Item Catalog (OIC). The OIC shall be the vehicle by which the County will purchase optional software, hardware and training.

The Contractor will invoice the County the total of the actual cost of the OIC item plus a 10% handling charge on the actual cost of such OIC item. This handling charge represents the Contractor's administrative and procurement cost associated with the acquisition of the OIC item on behalf of the County.

The County may, in its sole discretion, offer the Contractor an opportunity to establish the price and other terms for the procurement of optional hardware and software requested by the County. The County shall then determine, in its sole discretion, whether Contractor's proposed price and terms reflect the most favorable price and terms (including warranties and discounts) otherwise available. If Contractor's proposed price and terms are not the most favorable, Contractor shall have the opportunity to meet or beat the best price and terms discovered in the market by the County.

10.3.2. Desktop Applications Directory

The Optional Item Catalog includes the Desktop Applications Directory (DAD), which is a list of Desktop Applications supported by the Contractor. The baseline number of Desktop Applications in the DAD shall be four hundred and seventy-five (475).

It is the intent of the Parties to reasonably limit the Desktop Applications in the DAD. The Parties will determine the monthly average number of Desktop Applications in the DAD on December 31st of each Contract Year. Should the monthly average number of Desktop Applications exceed or fall below the baseline, the Parties agree to adjust the Fee for each Resource Unit in the Desktop Computing Services for the upcoming Contract Year as follows:

Desktop Applications in the DAD	**Fee added to or subtracted from each Resource Unit Fee in "Desktop Computing**
291-390	- $0.50
391-475	0
476-540	+ $0.50

Whether a Desktop Application is to be counted toward the DAD shall be determined by the County in its sole discretion based on various factors including but not limited to:

- Desktop Application executes solely on the desktop
- Desktop Application is a unique application, not just a different version
- Desktop Application is not a driver or other Software required to enable accessory hardware to properly operate or to install or delete other applications
- Desktop Application is not a font or a font set
- Desktop Application is not management Software, tools or utilities that the Contractor installs to provide the Services
- Desktop Application is not part of the Laptops, Desktops, Tablets and County Retained Devices

10.3.3. Addition to Optional Item Catalog

For any and all Services related to the addition of hardware that requires testing, as approved by the Catalog Review Board, or software to the Optional Item Catalog, Contractor shall perform any and all such Services pursuant to a Service Request submitted by County for a one-time

Resource Unit Fee per Schedule 16.1-1. Contractor shall be responsible for any and all costs associated with such activities beyond the Resource Unit Fee.

10.3.4. Updates to Desktop Application Directory Software

For any and all Services related to version updates to the Desktop Applications listed in the Optional Item Catalog, Contractor shall perform any and all such Services pursuant to a Service Request submitted by County for a one-time Resource Unit Fee per Schedule 16.1.-1. Contractor shall be responsible for any and all costs associated with such activities for such application beyond the Resource Unit Fee.

10.4. Electronic Signature Services

This section pertains to the Fees associated with Section 4.5.2.12 – Electronic Signature Services in Schedule 4.3 and listed in Exhibit 16.1-1.

The Electronic Signature Resource Unit (RU) Fee shall apply when a County user sends an agreement that requests at least one Adobe electronic signature (e-signature). This is referred to as an Adobe e-signature transaction. County will be charged the RU Fee listed in Exhibit 16.1-1 for each Adobe e-signature transaction.

10.5. Digital Signage Services

This section pertains to the Digital Signage Resource Unit (RU) associated with the services described in Schedule 4.3 Section 4.13, Digital Signage Services, and listed in Exhibit 16.1-1, Fees Summary by Resource Unit.

The Digital Signage Services RU is a three-year subscription commitment. When a County department purchases a subscription(s), they are authorizing to be billed the monthly RU Fee from the month that the subscription(s) was activated by Contractor through to the end of the three-year commitment. Contractor shall notify department no later than three months prior to end of subscription term and verify whether subscription is to be terminated or renewed. If the latter, Contractor will renew for a new three-year period and install new hardware device.

10.6. Survey Solution Support Services

This section pertains to the Fees associated with Section 4.16 in Schedule 4.3 and listed in Exhibit 16.1-1. The Survey Solution Support Services Resource Unit (RU) Fee shall apply only for County

users who have been assigned the role of Administrative User in SurveyMonkey, per an authorized Service Request.

10.7. Electronic File Sharing Services

This section pertains to the Electronic File Sharing Services Resource Unit (RU) associated with the services described in Schedule 4.3 Section 4.12, File Sharing Services, and listed in Exhibit 16.1-1, Fees Summary by Resource Unit.

The Electronic File Sharing Services provides for the following user types in the Box solution:

- County Staff
- Customer – member of the public as Unmanaged User
- Vendor – Third-party County vendor as Unmanaged User
- ITO Staff

Unmanaged users are unpaid personal accounts used to collaborate on the County-owned content and are within County's managed domain. Unmanaged users do not belong to the County electronic file sharing enterprise and their accounts are unlicensed. For clarity, managed County user folder(s) or file(s) that are shared with unmanaged users retain the same security, permissions, retention rules that are established by the managed County user. However, any free Unmanaged user has the ability to set up their own private folders, upload and share content with other users (internal and external) without being constrained by the enterprise settings that have been established by the County. Additionally, the County administrator(s) are not able to see the user activity, or any reports on the user.

The County will be charged the RU Fee listed in Exhibit 16.1-1 only for users assigned the "County Staff" role.

11. NETWORK SERVICES

This section pertains to the Fees associated with Section 5 – Network Services in Schedule 4.3 and listed in Exhibit 16.1-1.

11.1. Voice Services

This section pertains to the Fees associated with Section 5.7 – Voice Services in Schedule 4.3 and listed in Exhibit 16.1-1.

11.1.1. Voice Calls

County shall be billed for voice calls using the applicable Resource Unit based on the definitions and billing method set forth below.

Resource Unit	Definition	Billing Method
Calls: On-Net	Calls placed between County Locations	Per second
Calls: Off-Net Local	Calls placed from County Locations to Non-County locations with 619, 858, 442 and 760 prefix	Per second
Calls: Off-Net Long Distance	Calls placed from County Locations to Non-County locations within California outside of area codes 619, 858, 442 and 760 prefix.	Per second
Calls: Off-Net Long Distance	Calls placed from County Locations to Non-County locations outside California buy within United States and its territories.	Per second
Calls: International	Calls placed from County Locations to Non-County locations outside the United States and its territories.	Per second
Calls: Toll Free 800 Service (San Diego & Imperial)	Calls that are placed by the public to County Toll Free 800 numbers within San Diego and Imperial Counties.	Per second
Calls: Toll Free 800 Service	Calls that are placed by the public to County Toll Free 800 numbers outside San Diego and Imperial Counties but within California.	Per second
Calls: Toll Free 800 Service	Calls that are placed by the public to County Toll Free 800 numbers outside California but within United States and its territories.	Per second
Calls: Casual Use	Includes collect calls, person to person calls, person to person collect calls, remote calls, operator assistance calls, 3rd party calls, dial one calls, dedicated calls and other miscellaneous calls.	Per second
Calls: Conference	Calls placed to a conference bridge line.	Per second
Calls: Directory	Calls placed to obtain a listed telephone directory number.	Per call

11.1.2. Pay Phone

A Pay Phone located at County facilities as required by statute shall be billed at a flat monthly Resource Unit Fee per Exhibit 16.1-1.

11.1.3. Interactive Voice Services

County will be charged the applicable Interactive Voice Services (IVS) Resource Unit Fee based on the IVS components deployed for IVS application, as described in Schedule 4.3, Section 5.17.3. Tiered pricing (i.e., Small, Medium, and Large) will be based on the higher tier of the IVS Components deployed based on the table below.

Resource Unit	**IVS Component Deployed**
Interactive Voice Services - Small	Any of the following: • Automated Call Distribution • Auto Attendant • Call Management System
Interactive Voice Services - Medium	Any of the following: • Automated Call Recording • Virtual Wallboards • Agent Softphone
Interactive Voice Services - Large	Any of the following: • Interactive Voice Response • Short Message Service • Work Force Management • Physical Wallboards

11.1.4 Virtual Phone Advanced Features

County shall be billed the Virtual Phone Services – Microsoft (MS) Teams Advanced Features monthly Resource Unit for each active call flow in Microsoft Teams. In addition, the designated low org of each call flow shall be billed for the applicable number of MS Resource Account (RA) licenses associated with the call flow. MS Teams RA licenses requires an annual commitment and may not be terminated during its commitment term.

In Microsoft Teams, all auto attendants and call queues within a call flow require a RA, which is associated with a Microsoft Teams Phone RA license to ensure they are correctly identified by the system and properly function, regardless of whether the RA will be assigned a telephone number.

11.2. Network Access

This section pertains to the Network Access Resource Units associated with the services described in Schedule 4.3 Section 5 – Network Services and listed in Exhibit 16.1-1.

Devices, services and County users accessing the County network are subject to a Network Access Resource Unit Fee based on technology(s) through which network is accessed:

- Network Access - Static Wired – Device or service accesses County network at a County location through a wired connection only.
- Network Access - Wired/Wireless – County user accesses County network from a County location through a wired connection or Wireless Access Point connection.
- Virtual Private Network (VPN) Level 1 – Optional service that is an add-on to the Network Access - Wired/Wireless access capability.
- Virtual Private Network (VPN) Level 2 – Optional service that is an add-on to the Network Access - Wired/Wireless access capability.

The Network Access Resource Units are bundled; therefore, the monthly Fee applied to each resource unit is based on the total volume of the bundle.

11.3. Remote Site Redundancy for Key County Sites

At the County's option, on a site-by-site basis, during Years 1 through 4, Contractor shall provide a secondary circuit, at no additional monthly recurring cost to the County, to as many as fifteen sites provided that the County pays the fees associated with special construction costs for each Key site.

11.4. Remote Site Redundancy for T-1 Site

The County may elect, on a site-by-site basis, Contractor shall provide a secondary circuit based on LTE or like technology, at no additional monthly recurring cost to the County, provided that the County pays the fees associated with and special construction costs, if needed.

11.5. New Site Installation Services

This section pertains to the New Site Installation Resource Units (RUs) associated with the services described in Schedule 4.3 Section 5.16, New Site Installation Services, and listed in Exhibit 16.1-1, Fees Summary by Resource Unit.

The Site Type is determined by the number of Cable Drops, as defined in Section 5.16 of Schedule 4.3,

Operational Services, to be installed at the New Site. The Cable Drop threshold levels for each Site type are also described in Section 5.16 of Schedule 4.3, Operations Services.

The Fees associated with establishing a new County Site consists of two parts:

1. **New Site Install Fixed Component RU Fee** – This Fee applies to all New Site installations and covers all of the one-time activities required to be performed by the Contractor to establish the New Site as listed in Schedule 4.3, Operations Services.

   The New Site Install Fixed Component RU Fee is determined by the Site Type:

Site Type	Resource Unit
I	New Site Install– Type I Fixed Component
II	New Site Install– Type II Fixed Component
III	New Site Install– Type III Fixed Component
IV	New Site Install– Type IV Fixed Component
V	New Site Install– Type V Fixed Component
VI	New Site Install– Type VI Fixed Component

2. **New Site Install Variable Component RU Fee** – These set of Fees apply to the activities, as set forth in Schedule 4.3, Operations Services, required to install the cabling infrastructure in a New Site.

   The County has the option of either utilizing the Contractor to perform any or all these activities or contracting with a Third Party directly.

   There are five New Site Install Variable Component RUs related to a Site Type, each representing the cost associated with the deployment of the component of infrastructure per Site Type:

   - New Site Install Variable Component – Cable Drop
   - New Site Install Variable Component – Main Distribution Frame (MDF)
   - New Site Install Variable Component – Intermediate Distribution Frame (IDF)
   - New Site Install Variable Component – Back Bone cable (BB)
   - New Site Install Variable Component – Project Management (PM)

   The County will only be billed for applicable New Site Install Variable Components if Contractor is selected to perform such activities. The process to determine the total New Site

Install Variable Component RU Fee consists of:

1. Projection of the number of Cable Drops to be deployed in the New Site to determine the Site Type;
2. Assessment of the Variable Components required to support the installation based on Site Type.
3. By submitting a Service Request, the County may select a larger Variable Component (such as an MDF or IDF) than that recommended based on assessment. Additionally, if technical requirements change during installation, County will be notified of any required modification of the previously assessed RU Fee.

If the County opts to procure cabling installation services outside the Agreement:

1. Six months after the Turnover Date, a final accounting of number of Cable Drops installed to that point will be determined. If the number of Cable Drops exceeds the thresholds for the previously assessed Site Type by 10%:
    a. The applicable RU Fees for the additional Cables Drops shall be applied.
    b. If applicable, the Fixed and Variable Component charges shall be adjusted to the new Site Type;
2. Standards for these infrastructure components will be provided in the form of Cabling Standards document. Once completed, any defect in workmanship or materials found in wiring during the length of the warranty period granted to the County by their vendor, will be either: 1) referred to the County for resolution with their vendor or 2) repaired by the Contractor team. Any repairs performed by the Contractor team will be billable to the County through a Service Request.

11.6. Zoom Video Support Conferencing Services

This section pertains to the Zoom Video Support Conferencing Services Resource Unit (RU) associated with the services described in Schedule 4.3 Section 5.9, Video Conferencing Services, and listed in Exhibit 16.1-1, Fees Summary by Resource Unit.

The Zoom Video Support Conferencing Services RU will cover the following activities performed and procured by the Contractor for the administration and support of all enterprise paid-for accounts through the three-year agreement with Zoom:

- Re-assignment of paid user licenses and management of any STOP IMARs for paid licenses that are no longer needed.

- Resolution of Break/Fix incident tickets/calls for paid user licenses.
- Generation and posting of a monthly Schedule 5 report of Zoom accounts. Reporting of free accounts will also be included and will list free and paid accounts of users by low org. The report will be titled Zoom Users – Free and Paid Accounts by Low Org. This report will be the standard report generated from the Zoom portal.

Zoom licenses are not included in the Zoom Video Support Conferencing Services RU and must be acquired separately through OIC.

11.7. Mobility Services

This section pertains to the Mobility Services Resource Units (RUs) associated with the services described in Schedule 4.3 Section 5.18 - Mobility Services, and listed in Exhibit 16.1-1, Resource Unit Price Summary.

11.7.1. Mobile Devices in the Optional Item Catalog (OIC) – AT&T shall make mobile devices and mobile WiFi routers available for one-time purchase from the OIC in conjunction with the Mobility Services RUs.

11.7.2. FirstNet Mobility Services RU Fee – This Fee applies to mobile devices purchased from the OIC and to any eligible County mobile device that is enrolled for this service. This RU covers the following services provided by AT&T: Unlimited voice, text, and data service; FirstNet enabled service for all County users; and Free calling to Mexico and Canada.

11.7.3. FirstNet Mobility Services – Tethered – This Fee applies to mobile devices purchased from the OIC and to any eligible County mobile device that is enrolled for this service. This RU covers the following services provided by AT&T: Unlimited voice, text, and data service; FirstNet enabled service for all County users; Tethering Capability; and Free calling to Mexico and Canada.

11.7.4. Mobility Services – Hot Spot – This Fee applies to WiFi devices purchased from the OIC and covers the following services provided by AT&T: Unlimited data access for the mobile Wi-Fi router.

The Mobility Services RUs are not bundled; therefore, the monthly Fee applied to each RU is based on the individual volumes.

12. DATA CENTER SERVICES

This section pertains to the Fees associated with Section 6 – Data Center Services in Schedule 4.3 and listed in Exhibit 16.1-1.

12.1. Infrastructure Services

Contractor shall administer and manage the infrastructure environment to meet the requirements described in Schedule 4.3, Section 6.8. County will be charged a fixed monthly Resource Unit Fee for this service, as listed in Exhibit 16.1-1. This Resource Unit Fee includes the cost of hardware, software and labor associated with administering the environment as described in Exhibit 16.1-2.

12.2. Development and Test Services

12.2.1. Break/Fix Environment for Applications Maintenance & Operations (M&O)

Contractor shall administer and manage data center and infrastructure environment for the break/fix environment for Applications M&O to meet the requirements described in Schedule 4.3, section 6.9 and 7.2.2. County will be charged a fixed monthly Resource Unit Fee for this service, as listed in Exhibit 16.1-1. This Resource Unit Fee includes the cost of servers and storage associated with administering the environment.

12.2.2. Test/Development Environment for Applications Development

Contractor shall administer and manage data center and infrastructure environment for the test/development environment for Applications Development to meet the requirements described in Schedule 4.3, section 6.9 and 7.3.2. County will be charged a fixed monthly Resource Unit Fee for this service, as listed on Exhibit 16.1-1. This Resource Unit Fee includes the cost of servers and storage associated with administering the environment.

12.3. Storage and Data Management Services

This section pertains to the Fees associated with Section 6.12 – Storage and Data Management Services in Schedule 4.3 and listed in Exhibit 16.1-1.

Billing for Storage Services is as follows:

- Attached Storage – actual usage and 20% of the actual usage

- Storage - Primary Tier – actual usage and 20% of the actual usage
- Storage - Secondary Tier – actual usage and 20% of the actual usage
- Storage - Archive Tier – actual usage and 20% of the actual usage
- Storage - Immutable Tier – flat rate fee
- Storage - DPC – flat rate fee

Ad Hoc circumstances where an intermediate snapshot needs to be taken on a regular basis in order to facilitate backups and maintain application performance, will be considered a billable activity only after review and approval by the CIO or designee.

12.4. Cloud Services

This section pertains to the Fees associated with Cloud Services infrastructure support for applications hosted in either Amazon Web Services (AWS) or Microsoft Azure (MS Azure). Contractor shall administer and manage AWS and MS Azure to meet the requirements described in Schedule 4.3 and Schedule 4.8. Contractor will bill the County the applicable fixed monthly Resource Unit Fee for this service, as listed in Exhibit 16.1-1 and described below:

12.4.1. Cloud Infrastructure as a Service (IaaS) is for the support services provided by Contractor for each Infrastructure as a Service (IaaS) instance in the AWS and MS Azure clouds. Contractor shall provide the following support for IaaS: Software License / Maintenance (Operating System, Monitoring, Patching, Discovery, Antivirus); Build; Monitoring; Patching; Quality Control; Problem/Incident/Change Management; Upgrades; Decommission; Tech Refresh; Tools Management/Configuration; Server Security; Support to Applications, Service Level support; and Support to Architecture and Engineering.

12.4.2. Cloud Platform as a Service (PaaS) is for the support services provided by Contractor for each Platform as a Service instance in the AWS and MS Azure clouds. Contractor shall provide the following support for PaaS: Software License / Maintenance (Monitoring and Discovery); Build; Monitoring; Quality Control; Problem/Incident/Change Management; Decommission; Tools Management/Configuration; Server Security; Support to Applications, Service Level support; and Support to Architecture and Engineering.

12.4.3. Netbackup Solution AWS is for the daily backup/replication of AWS West Commercial tenant and the AWS East Commercial tenant for disaster recovery purposes. Contractor shall provide both licensing and support. Contractor will bill AWS backup storage associated with Netbackup Solution AWS plus a markup of 5% on a monthly basis.

12.4.4. Contractor will bill the County for AWS and MS Azure services consumed by business applications (e.g., compute, storage, database) plus a markup of 5% on a monthly basis.

12.4.5. Contractor will bill the County for AWS services associated with providing Core services in both AWS GovCloud and AWS Commercial Cloud plus a markup of 5% on a monthly basis. AWS services are limited to the following Core Services: Logging (CloudTrail), Monitoring (CloudWatch), Network Foundation (VPC), Security (GuardDuty, SecurityHubs, SecretsManager), Governance (AWSConfig), Directory Services (AWS DirectoryService), Compute (EC2), Database (RDS), Storage (S3, FSX, EBS), and Supporting Services (SNS, ELB, APIGateway, etc.)

Contractor will also bill the County for the services provided by AWS and MS Azure plus a markup of 5% on a monthly basis. These services are based on consumption based and therefore variable.

12.5. Low Code Application Platform – Outsystems

This section pertain to the Low code Application Platform – Outsystems Resource Unit (RU) associated with the services described in Schedule 4.3, Section 6.7.1 and listed in Exhibit 16-1-1, Fees Summary by Resource Unit.

12.5.1. The Low Code Application Platform – Outsystems RU is based on the Outsystems solution. The County will be charged the RU Fee listed in Exhibit 16.1-1 only for the internal County users and will provide access to unlimited number of applications within the platform. Enterprise licenses for external users will be charged separately.

13. APPLICATIONS SERVICES

13.1. Application Maintenance and Operations Services

See Exhibit 16.1-5b for details.

13.2. Application Development Services

13.2.1. Procurement of Applications Development

The County can procure Applications Development services for one-time IT Work through Contractor via any of the methods described below. If the resulting solution requires additional software licensing or hardware not already covered by the Agreement, this shall be handled through existing language in the Agreement for third-party agreements.

13.2.2. Contractor Developed

Per County Service Request, Contractor shall develop and price a solution based on a Statement of Work. Solution may be firm fixed price or time and materials based using the Resource Units in Exhibit 16.1-1 and the Labor Categories in Exhibit 16.1-4.

13.2.3. Pre-Approved Vendors

Per County Service Request, Contractor shall conduct a competitive procurement amongst the vendors on the pre-approved vendors list (maintained in the Standards and Procedures Manual), soliciting a priced solution based on a Statement of Work agreed to by both the County and Contractor. This activity is within the scope of the Contract and Acquisition Management Services.

13.2.4. Request for Proposal

Per County Service Request, Contractor shall conduct a competitive Request for Proposal (RFP) procurement process for a priced solution based on a Statement of Work agreed to by both the County and Contractor. County will be charged the Acquisition Manager Resource Unit Fee on an hourly basis as listed on Exhibit 16.1-1 should this effort require resources beyond what is provided in Contract and Acquisition Management Services.

13.2.5. Firm Fixed Price Projects

The County can request a firm fixed price (FFP) for certain IT work. Projects eligible for FFP work requests will be one-time efforts with specific time frames, scopes of work and defined deliverables. A project may include both Contractor and Third Party labor cost; Contractor labor cost only; and/or required hardware costs not already apart of the Agreement. Software licensing costs can be handled through existing language in the Agreement.

The County will provide a Statement of Work (SOW) to allow Contractor to adequately determine the requirements and costs associated with the project. The SOW will contain the project scope, project management requirements, reporting requirements, deliverables and schedule requirements, and validation and acceptance criteria, as well as specific warranty requirements (if applicable) and any terms that are different than contained in the underlying Agreement. The County may choose to require a performance bond or some other security vehicle depending upon the cost and scope level of the project being considered. The County will also establish as a part of the SOW the payment terms for the particular project, including performance and/or value-based payment methodologies. In some instances, the County may identify some terms in the underlying Agreement that may not apply to a given FFP Service Request and any exclusions, will be negotiated prior to final County approval of the FFP Service Request. The payment terms and SOW shall encompass the tasks required for the resulting solution to be included immediately after the conclusion of the project in the Applications Portfolio and Applications Maintenance and Operations Services. All aspects of the finalized SOW must be agreed to by both the County and Contractor prior to execution of the FFP Service Request.

FFP Service Request will be issued accordingly based on County selected procurement method as described in Section 13.2.1. Regardless of selected method, FFP Service Request will be subject to the requirements as called out in the Agreement for such documents. As with all work requests, appropriate cost breakdowns will be required from Contractor for review by the County.

Negotiations may be initiated by either party with respect to requirements, pricing or any other aspect of the project at any time after the submission of the SOW by the County until such time as the Service Request has been signed off and approved by both Contractor and the County. Any changes in project scope must include the proposed impact to pricing and schedule, which will be negotiated and mutually agreed to by both parties.

14. SPECIAL SERVICE LEVELS

This section pertains to the Fees associated with Schedule 4.8-1 and listed in Exhibit 16.1-1.

14.1. Registrar of Voters

The Special Service Level (SL) Support for Registrar of Voters (ROV) shall be billed at a pro-rated daily Resource Unit Fee per Exhibit 16.1-1. An authorized Service Request from ROV shall detail the start and end date of Special SL Support.

14.2. Treasurer-Tax Collector

The Special Service Level (SL) Support for Treasurer-Tax Collector (TTC) shall be billed as follows:

14.2.1. Fixed Price Event Coverage – Tax Collection

A one-time Resource Unit (RU) Fee for Special SL Support shall be billed per Tax Collection. The RU Fee covers a five (5) day period that is selected by TTC and detailed in the Service Request.

14.2.2. Fixed Price Event Coverage – Tax Sale

A one-time RU Fee for Special SL Support shall be billed per Tax Sale. The RU Fee covers a five (5) day period that is selected by TTC and detailed in the Service Request.

14.2.3. Special SL Support Daily Coverage

A daily RU Fee for Special SSL Support beyond the five (5) days included in the Fixed Price Event Coverage shall be billed if invoked by TTC. An authorized Service Request from TTC shall detail the start and end date of additional Special SL Support period.

14.3. Assessor / Record / County Clerk (ARCC) Acclaim

The Special Service Level (SL) Support for ARCC Acclaim shall be billed as follows:

14.3.1. Fixed Price Event Coverage – ARCC Month End

A Resource Unit (RU) for Special SL Support for ARCC Acclaim shall be billed per ARCC Month End Event. Due to the nature of the ARCC Month End Event, it will be billed automatically on every billing cycle. The Resource Unit Fee covers the last two business days of each month.

14.3.2. Fixed Price Event Coverage – ARCC Holiday Event

An RU for Special SL Support for ARCC Acclaim shall be billed per ARCC Holiday Event, if invoked. The Resource Unit Fee covers the business day before and business day after a County holiday.

14.3.3. Special SL Support Daily Coverage

ARCC may elect to invoke Special SL support beyond the days included in the Fixed Price Event Coverage. Should this be the case, the ARCC Special Support Daily Coverage rate will be charged for each additional day.

14.3.4. Immediate Response and Escalated Priority

Immediate Response and Escalated Priority apply to Applications as well as Infrastructure framework efforts related to e-Recording regardless of whether those efforts are being paid for via the Fixed Price Event Coverage, Special Support Daily Coverage, or by a separate Applications work request.

14.3.5. Application Support

Although the Special SL Support applies to work performed by the Applications Framework, payment for Application Services is provided on a time and materials basis under labor rates stated in the Agreement and is not part of the SL billing.

END OF SCHEDULE

Exhibit 16.1-1 – Resource Unit Price Summary

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Contract and Acquisition Management Services	****Schedule 4.3 Section 2.3	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 211,810.14	$ 2,541,721.63	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Integrated Asset Management Services	Schedule 4.3 - Section 2.4	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 112,804.78	$ 1,353,657.35	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Billing Management Services	Schedule 4.3 - Section 2.5	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 41,890.53	$ 502,686.31	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Security Management Services	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 240,747.14	$ 2,888,965.74	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Secure Internet Access	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 27,100.00	$ 325,200.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Malware Protection	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 5,062.50	$ 60,750.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Enterprise Application Access	Schedule 4.3 Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 75,117.37	$ 901,408.44	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Multi-Factor Authentication Service	Schedule 4.3 Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 42,152.00	$ 505,824.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Delivery Management Services	Schedule 4.3 - Section 2.7	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 197,508.06	$ 2,370,096.70	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Project Management Services	Schedule 4.3 - Section 2.9	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 133,967.13	$ 1,607,605.52	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Integration and Testing Services	Schedule 4.3 - Section 2.10	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 36,346.87	$ 436,162.42	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Incident Management Services	Schedule 4.3 - Section 2.11	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 3,316.47	$ 39,797.66	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Problem Management Services	Schedule 4.3 - Section 2.12	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 3,316.47	$ 39,797.66	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Change Management Services	Schedule 4.3 - Section 2.13	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 9,310.92	$ 111,731.04	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Release Management Services	Schedule 4.3 - Section 2.14	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 10,477.58	$ 125,731.01	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Configuration Management	Schedule 4.3 - Section 2.15	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 18,074.33	$ 216,891.94	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Capacity Planning and Performance Management Services	Schedule 4.3 - Section 2.16	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 17,497.78	$ 209,973.37	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Disaster Recovery Management Services	Schedule 4.3 - Section 2.17	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 208,849.96	$ 2,506,199.50	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Identity Access Management Services	Schedule 4.3 - Section 2.18	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 147,777.10	$ 1,773,325.22	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Reporting Management Services	Schedule 4.3 - Section 2.19	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 73,993.82	$ 887,925.82	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Domain Name Management Services	Schedule 4.3 - Section 2.20	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 1,523.67	$ 18,284.04	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Business Analyst Services	Schedule 4.3 - Section 2.21	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 79,296.61	$ 951,559.34	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Chief Technical Architect Services	Schedule 4.3 - Section 2.22	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 18,188.23	$ 218,258.71	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Enterprise Applications Architect Services	Schedule 4.3 - Section 2.23	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 18,188.23	$ 218,258.71	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Innovation Management Services	Schedule 4.3 - Section 2.24	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 20,069.65	$ 240,835.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Desk Services	Schedule 4.3 - Section 3	Service Desk Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 198,226.81	$ 2,378,721.69	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Duo Hardware Token MFA	Schedule 4.3 - Section 4.5.2	End User Services	Account	Fixed Monthly Fee Per Unit		Specific	10	$ 5.28	$ 52.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Electronic Signature	Schedule 4.3 - Section 4.5.2	End User Services	Transaction	Fixed Fee Per Unit		Cumulative	25,000	$ 1.01	$ 25,250.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Desktop - 3D Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	396	$ 273.69	$ 108,381.24	$ 300.61	$ 285.75	$ 267.09	$ 261.40	$ 256.62	$ 251.92	3

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Desktop - Advanced Engineering Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3,228	$ 210.24	$ 678,654.72	$ 230.92	$ 219.51	$ 205.17	$ 200.80	$ 197.12	$ 193.52	4
Desktop - Advanced Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	112,776	$ 94.11	$ 10,613,349.36	$ 103.36	$ 98.26	$ 91.84	$ 89.88	$ 88.24	$ 86.62	4
Desktop - Engineering Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3,228	$ 111.13	$ 358,721.18	$ 122.06	$ 116.03	$ 108.45	$ 106.14	$ 104.20	$ 102.29	4
Desktop - Gold Engineering Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	44	$ 295.72	$ 13,011.68	$ 324.81	$ 308.76	$ 288.59	$ 282.44	$ 277.27	$ 272.20	4
Desktop - Mini Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	250	$ 64.96	$ 16,240.00	$ 71.35	$ 67.82	$ 63.39	$ 62.04	$ 60.91	$ 59.79	4
Desktop - Small Form Factor with Optical Drive	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	250	$ 64.96	$ 16,240.00	$ 71.35	$ 67.82	$ 63.39	$ 62.04	$ 60.91	$ 59.79	4
Desktop - Standard Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	112,776	$ 64.96	$ 7,325,928.96	$ 71.35	$ 67.82	$ 63.39	$ 62.04	$ 60.91	$ 59.79	4
Desktop - Scanner	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	528	$ 136.17	$ 71,897.76	$ 164.52	$ 155.54	$ 146.57	$ 143.58	$ 140.59	$ 137.60	4
Laptop - Engineering	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	900	$ 165.27	$ 148,743.00	$ 181.53	$ 172.55	$ 161.28	$ 157.85	$ 154.96	$ 152.12	3
Laptop - Ruggedized	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	636	$ 188.33	$ 119,777.88	$ 206.86	$ 196.64	$ 183.79	$ 179.88	$ 176.58	$ 173.35	3
Laptop - Standard	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	37,212	$ 86.55	$ 3,220,698.60	$ 95.07	$ 90.37	$ 84.46	$ 82.67	$ 81.15	$ 79.67	3
Laptop - Ultra Portable	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	10,392	$ 93.86	$ 975,424.30	$ 103.10	$ 98.00	$ 91.60	$ 89.65	$ 88.01	$ 86.40	3
Laptop - Ultra Portable 2in1	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	372	$ 106.48	$ 39,611.68	$ 116.96	$ 111.18	$ 103.92	$ 101.70	$ 99.84	$ 98.02	3
Tablet - Convertible	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3,420	$ 95.28	$ 325,869.57	$ 104.66	$ 99.49	$ 92.99	$ 91.01	$ 89.34	$ 87.71	3
Tablet - Ruggedized	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	360	$ 209.83	$ 75,538.80	$ 230.48	$ 219.08	$ 204.77	$ 200.41	$ 196.74	$ 193.14	3
Tablet - Surface Pro	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3,480	$ 106.92	$ 372,076.38	$ 117.44	$ 111.63	$ 104.34	$ 102.12	$ 100.25	$ 98.42	3
Laptop - Standard LTE	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	100	$ 109.10	$ 10,910.00	$ 119.83	$ 113.91	$ 106.47	$ 104.20	$ 102.29	$ 100.42	3
Tablet - Surface Pro LTE	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	100	$ 138.02	$ 13,802.00	$ 151.60	$ 144.10	$ 134.69	$ 131.82	$ 129.41	$ 127.04	3
Early Refresh - Desktop	Schedule 4.3 - Section 4.5.4	End User Services	Month	Fixed Fee Per Unit		Cumulative	10	$ 34.00	$ 340.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Early Refresh - Mobile PC	Schedule 4.3 - Section 4.5.4	End User Services	Month	Fixed Fee Per Unit		Cumulative	30	$ 47.00	$ 1,410.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
County Retained Device	Schedule 4.3 - Section 4.7.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	48	$ 103.09	$ 4,948.32	$ 113.23	$ 107.64	$ 100.61	$ 98.46	$ 96.66	$ 94.89	3
Desktop - DCSS	Schedule 4.3 - Section 4.7.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	6,432	$ 36.23	$ 232,999.20	$ 39.79	$ 37.82	$ 35.35	$ 34.60	$ 33.97	$ 33.34	n/a
Laptop - DCSS	Schedule 4.3 - Section 4.7.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	180	$ 44.31	$ 7,975.80	$ 48.67	$ 46.26	$ 43.24	$ 42.32	$ 41.55	$ 40.79	n/a
Mobile Device Support Services – Intune	Schedule 4.3 - Section 4.8	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	57,000	$ 7.51	$ 428,070.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Printer - Color Network Workgroup - Large Format (CNWP-LF)	Schedule 4.3 - Section 4.11	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	528	$ 165.77	$ 87,525.50	$ 182.08	$ 173.08	$ 161.77	$ 158.33	$ 155.43	$ 152.59	4
Printer - Color Network Workgroup - Standard Format (CNWP)	Schedule 4.3 - Section 4.11	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	2,328	$ 67.57	$ 157,311.11	$ 74.22	$ 70.55	$ 65.94	$ 64.54	$ 63.36	$ 62.20	4
Printer - Monochrome Network Workgroup - Standard Format (MNWP)	Schedule 4.3 - Section 4.11	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	8,964	$ 60.49	$ 542,223.40	$ 66.44	$ 63.16	$ 59.03	$ 57.77	$ 56.72	$ 55.68	4
Printer - Monochrome Network High Volume - Large Format (MNWP-LF-H)	Schedule 4.3 - Section 4.11	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	312	$ 158.88	$ 49,571.83	$ 173.17	$ 165.87	$ 155.98	$ 153.12	$ 150.32	$ 147.57	4

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Printer - Monochrome Network Workgroup - Large Format (MNWP-LF)	Schedule 4.3 - Section 4.11	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	264	$ 97.43	$ 25,721.52	$ 107.17	$ 101.33	$ 95.48	$ 93.53	$ 91.58	$ 89.64	4
Electronic File Sharing Services	Schedule 4.3 - Section 4.12	End User Services	User	Fixed Monthly Fee Per Unit		Specific	1,212	$81.25 (101-250)	$ 98,475.00	$56.55 (251-500)	$47.83 (501 1000)	$42.18 (1000+)	n/a	n/a	n/a	n/a
Digital Signage Services	Schedule 4.3 - Section 4.13	End User Services	Subscription	Fixed Monthly Fee Per Unit		Specific	2,400	$ 68.37	$ 164,088.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Survey Solution Support Services	Schedule 4.3 - Section 4.13	End User Services	Administrator	Fixed Monthly Fee Per Unit		Specific	360	≤60 Users $ 48.94	$ 17,618.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
A/V Conference Room - Large	Schedule 4.3 - Section 4.13	End User Services	Install	Fixed Fee Per Unit		Cumulative	1	$ 64,563.91	$ 64,563.91	n/a	n/a	n/a	n/a	n/a	n/a	n/a
A/V Conference Room - Medium	Schedule 4.3 - Section 4.13	End User Services	Install	Fixed Fee Per Unit		Cumulative	1	$ 34,671.93	$ 34,671.93	n/a	n/a	n/a	n/a	n/a	n/a	n/a
A/V Conference Room - Small	Schedule 4.3 - Section 4.13	End User Services	Install	Fixed Fee Per Unit		Cumulative	1	$ 25,004.76	$ 25,004.76	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Network Access - Static Wired	Schedule 4.3 - Section 5.5	Network Services	Device	Fixed Monthly Fee Per Unit	B2	Specific	27,708	$ 55.93	$ 1,549,831.71	$ 64.04	$ 59.85	$ 54.82	$ 53.72	$ 52.65	$ 51.59	n/a
Network Access - Static Wired (Library)	Schedule 4.3 - Section 5.6	Network Services	Device	Fixed Monthly Fee Per Unit	B2	Specific	120	$ 49.77	$ 5,972.40	$ 56.98	$ 53.25	$ 48.77	$ 47.80	$ 46.84	$ 45.91	4/5
Uninterrupted Power Supply Support Services	Schedule 4.3 - Section 5.5	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12	$ 110.00	$ 1,320.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Private Network Access - Level 1	Schedule 4.3 - Section 5.6	Network Services	Active Account	Fixed Monthly Fee per Unit		Specific	46,212	$ 9.40	$ 434,392.80	$ 10.72	$ 10.06	$ 9.21	$ 9.02	$ 8.84	$ 8.65	4
Virtual Private Network Access - Level 2	Schedule 4.3 - Section 5.6	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	20,952	$ 10.91	$ 228,586.32	$ 12.49	$ 11.67	$ 10.69	$ 10.48	$ 10.27	$ 10.06	n/a
Portal - External Users	Schedule 4.3 - Section 5.6	Network Services	User	Fixed Monthly Fee Per Unit		Specific	200	$ 8.00	$ 1,600.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Portal - Portfolio Application	Schedule 4.3 - Section 5.6	Network Services	Application	Fixed Monthly Fee Per Unit		Specific	0	$ 210.90	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Casual Use	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	6,167,520	$ 0.017359	$ 107,060.71	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Conference Bridge	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	53,415,060	$ 0.001337	$ 71,438.43	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Directory Assistance	Schedule 4.3 - Section 5.7	Network Services	Call	Fixed Fee Per Unit		Cumulative	233	$ 0.517658	$ 120.61	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: International	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	1,535,088	$ 0.002329	$ 3,575.52	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Local	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	762,100,578	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Toll	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	194,183,047	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Long Distance (CA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	112,254,258	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls Off-Net Long Distance (USA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	78,582,984	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: On-Net	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	0	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Toll Free 800 Service (CA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	91,282,130	$ 0.000334	$ 30,451.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Toll Free 800 Service (San Diego & Imperial)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	1,235,112,040	$ 0.000334	$ 412,079.10	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Toll Free 800 Service (USA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	127,834,956	$ 0.000334	$ 42,644.08	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Pay Phones	Schedule 4.3 - Section 5.7	Network Services	Phone	Fixed Monthly Fee Per Unit		Specific	36	$ 82.95	$ 2,986.20	n/a	n/a	n/a	n/a	n/a	n/a	n/a
GSMS Short Code Setup	Schedule 4.3 - Section 5.7	Network Services	Event	Fixed Fee Per Unit		Cumulative	1	$ 3,700.00	$ 3,700.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Mobile Device Support Services – Intune	Schedule 4.3 - Section 5.7	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 1,507.63	$ 18,091.56	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
GSMS Messages	Schedule 4.3 - Section 5.7	Network Services	Message	Fixed Fee Per Unit		Cumulative	1,680,000	$ 0.028	$ 47,040.00	0-10,000 Messages $0.00	10,000 - 100,000 Messages $0.33	100,001-500,000 Messages $0.28	500,001 + Messages $0.23	n/a	n/a	n/a
IP Conference Phone	Schedule 4.3 - Section 5.7.3	Network Services	Phone	Fixed Monthly Fee Per Unit		Specific	299	$ 59.72	$ 17,856.28	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Phone - Microsoft (MS) Teams Phone	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	36,000	$ 16.85	$ 606,600.00	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice-Avaya Legacy Support	Schedule 4.3 - Section 5.7.3	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 416,688.00	$ 5,000,256.00	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Analog Line	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	35,772	$ 47.55	$ 1,700,861.72	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Single-Line	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	29,088	$ 22.84	$ 664,369.92	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Multi-Line	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	137,400	$ 25.05	$ 3,441,870.00	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Mail	Schedule 4.3 - Section 5.7.3	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	159,060	$ 3.61	$ 574,273.68	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Mail to Email Services	Schedule 4.3 - Section 5.7.3	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	448	$ 1.72	$ 769.97	n/a	n/a	n/a	n/a	n/a	n/a	5
Cloud Access Security Broker	Schedule 4.3 - Section 5.8	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 15,450.12	$ 185,401.44	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Town Hall Services	Schedule 4.3 - Section 5.9	Network Services	Event	Fixed Fee Per Unit		Cumulative	0	$ 76,730.20	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Video Conferencing Services - Personal	Schedule 4.3 - Section 5.9	Network Services	System	Fixed Monthly Fee Per Unit		Specific	780	$ 315.70	$ 246,246.00							
Video Conferencing Services - Room System	Schedule 4.3 - Section 5.9	Network Services	System	Fixed Monthly Fee Per Unit		Specific	48	$ 895.13	$ 42,966.45	n/a	n/a	n/a	n/a	n/a	n/a	n/a
BlueJeans Video Conferencing Service	Schedule 4.3 - Section 5.9	Network Services	License	Fixed Monthly Fee Per Unit		Specific	360	$ 35.75	$ 12,870.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Webex Video Conferencing Services	Schedule 4.3 - Section 5.9	Network Services	Subscription	Fixed Monthly Fee Per Unit		Specific	102 (subscription / month)	$47.86 (≥102 subscriptions / month)	4881.72	n/a	$66.85 (≤ 102 subscriptions license / month)	n/a	n/a	n/a	n/a	n/a
Video Streaming - COC Chambers	Schedule 4.3 - Section 5.10	Network Services	System	Fixed Monthly Fee Per Unit		Specific	12	$ 1,210.00	$ 14,520.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Legislative Management Suite	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 3,630.00	$ 43,560.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Video Streaming and Archiving Services	Schedule 4.3 - Section 5.10	Network Services	System	Fixed Monthly Fee Per Unit		Specific	12	$ 7,210.62	$ 86,527.39	n/a	n/a	n/a	n/a	n/a	n/a	n/a
VoteCast	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 2,365.00	$ 28,380.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Engagement HQ	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed monthly fee per unit		Specific	12	$5,637.50	$ 67,650.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Wireless Access Point	Schedule 4.3 - Section 5.12	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	8,808	$ 160.18	$ 1,410,865.44	$ 183.39	$ 171.39	$ 156.77	$ 153.37	$ 149.85	$ 146.55	3
Network Access - Wire/Wireless	Schedule 4.3 - Section 5.12	Network Services	Active Account	Fixed Monthly Fee Per Unit	B2	Specific	179,304	$ 66.68	$ 11,955,647.14	$ 76.34	$ 71.35	$ 65.34	$ 64.04	$ 62.76	$ 61.50	n/a
3rd-Party Network Access - Category 1	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	36	$ 536.92	$ 19,329.25	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd-Party Network Access - Category 2	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	24	$ 544.44	$ 13,066.57	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd-Party Network Access - Category 3	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	60	$ 548.74	$ 32,924.58	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - IP Sec - 5 Mbps	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	120	$ 255.85	$ 30,702.11	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - IP Sec - 10 Mbps	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 427.31	$ 5,127.71	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (1 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 153.51	$ 1,842.13	n/a	n/a	n/a	n/a	n/a	n/a	5

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
3rd Party Network Access - Virtual Access (2 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 260.12	$ 3,121.38	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (3 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	24	$ 373.93	$ 8,974.21	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (4 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 473.32	$ 5,679.89	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (5 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	36	$ 613.55	$ 22,087.94	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (6-10 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 1,155.51	$ 13,866.17	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (20 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 1,907.15	$ 1,907.15	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (30 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 2,504.79	$ 2,504.79	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (40 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 2,879.77	$ 2,879.77	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (50 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 3,032.09	$ 3,032.09	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Microsoft Teams Rooms	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	168	$ 359.17	$ 60,340.56	n/a	n/a	n/a	n/a	n/a	n/a	n/a
External DNS Management	Schedule 4.3 - Section 5.14	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 15,265.83	$ 183,189.98	n/a	n/a	n/a	n/a	n/a	n/a	n/a
External DNS Management Enhancement	Schedule 4.3 - Section 5.14	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 28,373.54	$ 340,482.48	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type I Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 232,875.88	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 12,135.84	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 7,991.30	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 21,909.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 46,818.22	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type II Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 116,437.94	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 10,504.22	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 7,991.30	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 21,909.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,409.11	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type III Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 80,073.31	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 10,504.22	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 7,991.30	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 21,909.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
New Site Install - Type III Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 11,704.55	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type IV Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 67,793.32	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 8,872.60	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,134.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 21,909.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,852.28	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type V Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 16,791.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 8,872.60	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,134.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 21,909.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 3,745.46	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type VI Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 3,197.05	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 6,015.30	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,134.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 21,909.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 2,106.82	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Cable Drops	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 497.21	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Large	Schedule 4.3 - Section 5.17	Network Services	System	Fixed Monthly Fee Per Unit		Specific	96	$ 8,234.60	$ 790,521.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Medium	Schedule 4.3 - Section 5.17	Network Services	System	Fixed Monthly Fee Per Unit		Specific	12	$ 2,722.50	$ 32,670.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Small	Schedule 4.3 - Section 5.17	Network Services	System	Fixed Monthly Fee Per Unit		Specific	348	$ 687.50	$ 239,250.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Support for County Retained	Schedule 4.3 - Section 5.17	Network Services	System	Fixed Monthly Fee Per Unit		Specific	180	$ 616.58	$ 110,983.88	n/a	n/a	n/a	n/a	n/a	n/a	5
FirstNet Mobility Services	Schedule 4.3 - Section 5.18	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12,000	$31.49 ≥ 1000 per month	$ 377,880.00	$36.49 ≤ 999 per month	n/a	n/a	n/a	n/a	n/a	n/a
FirstNet Mobility Services - Tethered	Schedule 4.3 - Section 5.18	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12,000	$36.60 ≥ 1000 per month	$ 439,200.00	$41.6 ≤ 999 per month	n/a	n/a	n/a	n/a	n/a	n/a
Mobility Services Hot Spot	Schedule 4.3 - Section 5.18	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12	$ 25.58	$ 306.96	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Citrix Account	Schedule 4.3 - Section 6	Data Center Services	Account	Fixed Monthly Fee Per Unit		Specific	344	$ 20.68	$ 7,113.92	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Guest Server - Cloud IaaS	Schedule 4.3 - Section 6	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	48	$551.27	$ 26,460.96	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Virtual Guest Server - Cloud PaaS	Schedule 4.3 - Section 6	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	48	$413.45	$ 19,845.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Transaction	Schedule 4.3 - Section 6	Data Center Services	Third Party Transaction	Fixed Fee Per Unit		Cumulative	n/a	5% of invoice amount	**	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Clonetab Solution	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 6,211.24	$ 74,534.88	n/a	n/a	n/a	n/a	n/a	n/a	4
DIMSNET Solution	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 15,369.32	$ 184,431.84	n/a	n/a	n/a	n/a	n/a	n/a	4
Wild Fire Scanning Service	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 6,658.80	$ 79,905.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBackup Solution	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 107,963.65	$ 1,295,563.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Mainframe	Schedule 4.3 - Section 6.6	Data Center Services	CPU Hour***	Fixed Monthly Fee Per Unit		Specific	15,305	$ 96.63	$ 1,478,922.11	n/a	n/a	n/a	n/a	n/a	n/a	7
AS/400	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	12	$ 3,118.66	$ 37,423.94	n/a	n/a	n/a	n/a	n/a	n/a	5
Copia Fax Line	Schedule 4.3 - Section 6.7	Data Center Services	Fax Line	Fixed Monthly Fee Per Unit		Specific	12	$ 125.00	$ 1,500.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Low Code Application Platform - OutSystems	Schedule 4.3 - Section 6.7	Data Center Services	User	Fixed Monthly Fee Per Unit		Specific	5,000	≤5000 $54.06	$ 270,300.00	n/a	n/a	>5000 $42.00	n/a	n/a	n/a	n/a
Physical Server UNIX - Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	900	$ 4,878.56	$ 4,390,707.57	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server UNIX - Medium	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	720	$ 2,894.99	$ 2,084,390.98	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server UNIX - Small	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	330	$ 1,811.71	$ 597,864.53	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server UNIX - X-Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	72	$ 5,238.56	$ 377,176.32	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Wintel - Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	160	$ 1,676.75	$ 268,279.51	n/a	n/a	n/a	n/a	n/a	n/a	4
Physical Server Wintel - Medium	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	300	$ 1,167.08	$ 350,122.94	n/a	n/a	n/a	n/a	n/a	n/a	4
Physical Server Wintel - Small	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	400	$ 940.41	$ 376,164.77	n/a	n/a	n/a	n/a	n/a	n/a	4
Physical Server Wintel - X-Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	24	$ 1,960.86	$ 47,060.64	n/a	n/a	n/a	n/a	n/a	n/a	4
Virtual Guest Server - Linux	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	300	$ 646.88	$ 194,065.20	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Unix	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	160	$ 1,293.77	$ 207,002.88	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Windows	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	4,550	$ 616.08	$ 2,803,164.00	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Host Server - Windows / Linux	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	160	$ 5,328.61	$ 852,577.60	n/a	n/a	n/a	n/a	n/a	n/a	4
Physical Server UNIX - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	11	$4,976.63	$ 54,742.93	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Wintel - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	2	$1,862.82	$ 3,725.64	n/a	n/a	n/a	n/a	n/a	n/a	4
Virtual Guest Server - Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	63	$614.54	$ 38,716.02	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Unix - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	7	$ 1,229.08	$ 8,603.56	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Windows - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	8	$ 585.28	$ 4,682.24	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Host Server - Windows / Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	3	$ 5,062.18	$ 15,186.54	n/a	n/a	n/a	n/a	n/a	n/a	4
Oracle Exadata Services - Eighth Rack	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	12	$ 10,380.95	$ 124,571.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Oracle Exadata Services - Backup and Recovery	Schedule 4.3 - Section 6.7	Data Center Services	Used Terabyte	Fixed Monthly Fee Per Unit		Specific	0	$ 122.88	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata X8M - Production	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	12	$ 40,951.09	$ 491,413.08	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata X8M - Development / Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	12	$ 33,503.21	$ 402,038.49	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata X8M - Business Continuity	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	12	$ 41,268.64	$ 495,223.65	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Acclaim Riverbed	Schedule 4.3 - Section 6.8	Data Center Services	Riverbed	Fixed Monthly Fee Per Unit		Specific	72	$ 1,905.36	$ 137,185.92	n/a	n/a	n/a	n/a	n/a	n/a	4
Infrastructure Services	Schedule 4.3 - Section 6.8	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 325,304.45	$ 3,903,653.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Development & Test Services	Schedule 4.3 - Section 6.9	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 223,622.34	$ 2,683,468.08	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Fax	Schedule 4.3 - Section 6.10	Data Center Services	Account	Fixed Monthly Fee Per Unit		Specific	500	$ 38.28	$ 19,140.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
E-Mail Services	Schedule 4.3 - Section 6.10	Data Center Services	Active Account	Fixed Monthly Fee Per Unit		Specific	162,420	$ 5.24	$ 851,290.39	n/a	n/a	n/a	n/a	n/a	n/a	5
Attached Storage - WINTEL	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	38,826	$ 0.82	$ 31,837.32	$ 0.94	$ 0.87	$ 0.80	$ 0.78	$ 0.77	$ 0.75	n/a
Attached Storage - Unix	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	0	$ 1.07	$ -	$ 1.21	$ 1.13	$ 1.05	$ 1.03	$ 1.01	$ 1.00	n/a
Storage - Archive Tier	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	0	$ 0.30	$ -	$ 0.34	$ 0.31	$ 0.29	$ 0.29	$ 0.28	$ 0.28	n/a
Storage - Primary Tier	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	1,638,468	$ 0.74	$ 1,212,466.32	$ 0.85	$ 0.79	$ 0.72	$ 0.70	$ 0.69	$ 0.68	n/a
Storage - Secondary Tier	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	3,554,814	$ 0.52	$ 1,848,503.28	$ 0.60	$ 0.56	$ 0.50	$ 0.49	$ 0.48	$ 0.47	n/a
Attached Storage - AS/400	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit		Specific	1,920	$ 0.695	$ 1,334.40	n/a	n/a	n/a	n/a	n/a	n/a	7
Attached Storage - Mainframe	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit		Specific	13,286	$ 6.73	$ 89,414.78	n/a	n/a	n/a	n/a	n/a	n/a	7
Storage - Document Processing Center 1	Schedule 4.3 - Section 6.12	Data Center Services	Unit	Fixed Monthly Fee Per Unit		Specific	12	$ 16,579.20	$ 198,950.40	n/a	n/a	n/a	n/a	n/a	n/a	5
Storage - Document Processing Center 2	Schedule 4.3 - Section 6.12	Data Center Services	Unit	Fixed Monthly Fee Per Unit		Specific	12	$ 9,828.00	$ 117,936.00	n/a	n/a	n/a	n/a	n/a	n/a	5
Storage - Immutable Tier (1TB)	Schedule 4.3 - Section 6.12	Data Center Services	1 Terabyte	Fixed Monthly Fee Per Unit		Specific	144	$ 638.62	$ 91,961.38	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Storage - Immutable Tier (500GB)	Schedule 4.3 - Section 6.12	Data Center Services	512 Gigabyte	Fixed Monthly Fee Per Unit		Specific	120	$ 319.31	$ 38,317.24		n/a	n/a	n/a	n/a	n/a	n/a
Print per 1,000 images (Paper)	Schedule 4.3 - Section 6.14	Data Center Services	1000 Images	Fixed Fee Per Unit		Cumulative	4,318	$ 63.62	$ 274,719.02	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Microfiche Originals	Schedule 4.3 - Section 6.14	Data Center Services	Copy	Fixed Fee Per Unit		Cumulative	12,264	$ 1.20	$ 14,771.99	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Microfiche Duplicates	Schedule 4.3 - Section 6.14	Data Center Services	Copy	Fixed Fee Per Unit		Cumulative	41,964	$ 0.12	$ 4,846.84	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Fixed Price Applications Service Request	Schedule 16.1	Applications Services	Service Request	Fixed Fee Per Unit		Cumulative	n/a	n/a	**	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Transaction	Exhibit 4.3 - Section 2.3.1.4, Exhibit 16.1	Cross Functional Services	Third Party Transaction	Fixed Fee Per Unit		Cumulative	n/a	3% - 5% (Depending on product or service)	**	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Negotiation - Large	Exhibit 4.3 - Section 2.3.1.4, Exhibit 16.1	Cross Functional Services	Third Party Agreement	Fixed Fee Per Unit		Cumulative	n/a	$ 10,000.00	**	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Negotiation - Small	Exhibit 4.3 - Section 2.3.1.4, Exhibit 16.1	Cross Functional Services	Third Party Agreement	Fixed Fee Per Unit		Cumulative	n/a	$ 5,000.00	**	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Electronic Health Records Program Management Services	Schedule 4.3- Section 7.4	Applications Services	Month	Fixed Fee Per Unit		Specific	12	$ 55,000.00	$ 660,000.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Acquisition Manager	Exhibit 4.3 - Section 2.3.1.5, Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	4,160	$ 125.00	$ 520,000.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Architect	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	9,685	$ 162.82	$ 1,576,920.96	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	11,497	$ 98.57	$ 1,133,304.59	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - Advanced Technology	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	88,864	$ 132.21	$ 11,748,269.53	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - Associate	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	283	$ 70.00	$ 19,810.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - ERP Principal	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	3,700	$ 195.00	$ 721,500.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - Senior	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	42,938	$ 120.61	$ 5,178,671.26	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Test Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	3,783	$ 95.00	$ 359,385.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Test Lead	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,570	$ 126.40	$ 324,848.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Business Analyst	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,080	$ 113.77	$ 236,638.38	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Data Entry Clerk	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	400	$ 26.00	$ 10,400.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Database Administrator	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	20,545	$ 138.82	$ 2,851,960.38	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Desktop Engineer	Exhibit 16.1-4	End User Services	Hour	Fixed Fee Per Unit		Cumulative	55	$ 99.95	$ 5,497.25	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Gate Review Coordinator	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	160	$ 90.00	$ 14,400.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Innovation Core Team Member (Effective CY2)	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	**	$ 168.82	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Intern	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	800	$ 33.00	$ 26,400.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Junior Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	400	$ 33.00	$ 13,200.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Network Architect	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	120	$ 170.58	$ 20,469.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Network Engineer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	120	$ 110.17	$ 13,220.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Program Manager	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	897	$ 193.90	$ 173,928.96	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Project Manager	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	19,785	$ 155.34	$ 3,073,420.37	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Project Scheduler	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	1,494	$ 95.00	$ 141,930.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Curam Interface Architect	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,080	$ 270.00	$ 561,600.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Curam Business Analyst	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,080	$ 185.00	$ 384,800.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Network Engineer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	120	$ 153.01	$ 18,361.20	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Systems Analyst	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	29,295	$ 114.81	$ 3,363,348.65	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Web Designer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,449	$ 106.46	$ 260,720.19	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Curam Application Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	4,160	$ 195.00	$ 811,200.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Maintenance & Operations FFP (County)	Exhibit 16.1-5b	Applications Services	Year	Fixed Fee Per Unit		Specific	**	**	$ 9,482,333.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Maintenance & Operations FFP (Group)	Exhibit 16.1-5b	Applications Services	Year	Fixed Fee Per Unit		Specific	**	**	Not Exercised	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Maintenance & Operations FFP (Low Org)	Exhibit 16.1-5b	Applications Services	Year	Fixed Fee Per Unit		Specific	**	**	Not Exercised	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Optional Item Catalog (OIC) - Update	Exhibit 16.1 - Section 10.2	Catalog	Update	Fixed Fee Per Unit		Cumulative	12	$ 1,400.00	$ 16,800.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Optional Item Catalog (OIC) - Software Addition	Exhibit 16.1 - Section 10.3	Catalog	Add	Fixed Fee Per Unit		Cumulative	12	$ 2,450.00	$ 29,400.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Optional Item Catalog (OIC) - Hardware Addition	Exhibit 16.1 - Section 10.3	Catalog	Add	Fixed Fee Per Unit		Cumulative	12	$ 500.00	$ 6,000.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - Service Desk Framework	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - Application Services Framework	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - End User Services Framework	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - Network Services Framework	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - Data Center Services Framework	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - Cross Functional Services Framework	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Transition Services - Transition Completion	Schedule 2.1	Transition Services	Milestone	Fixed Fee Per Unit		Specific	1	$ 7,212,700.17	$ 7,212,700.17	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
ARCC Special Service Level Support Services - Event Coverage	Schedule 4.8-1	Special Service Level Requirements	Event	Fixed Fee Per Unit		Cumulative	22	$ 2,793.52	$ 61,457.44	n/a	n/a	n/a	n/a	n/a	n/a	n/a
ARCC Special Service Level Support Services - Daily Support	Schedule 4.8-1	Special Service Level Requirements	Day	Fixed Fee Per Unit		Cumulative	5	$ 1,396.76	$ 6,983.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Registrar of Voters	Schedule 4.8-1	Special Service Level Requirements	Day	Fixed Fee Per Unit		Cumulative	99	$ 441.98	$ 43,756.02	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Tax Sale Event	Schedule 4.8-1	Special Service Level Requirements	Event	Fixed Fee Per Unit		Cumulative	1	$ 5,748.75	$ 5,748.75	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Tax Collection Event	Schedule 4.8-1	Special Service Level Requirements	Event	Fixed Fee Per Unit		Cumulative	2	$ 11,521.35	$ 23,042.70	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Special Support Daily Coverage	Schedule 4.8-1	Special Service Level Requirements	Day	Fixed Fee Per Unit		Cumulative	50	$ 180.00	$ 9,000.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Labor	Schedule 4.3 - Section 2.17	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	0	$ 22,621.27	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Infrastructure	Schedule 4.3 - Section 2.17	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	0	$ 56,744.73	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Small Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 55.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Medium Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 100.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Large Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 387.48	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR X-Large Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 483.31	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Medium Solaris - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 193.14	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Large Solaris - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 556.21	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR X-Large Solaris - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	1 Terabyte	Fixed Monthly Fee Per Unit		Specific	0	$ 669.29	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR VTL Based Storage - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 139.39	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Small Virtual - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 128.22	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Medium Virtual - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 144.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Large Virtual - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 171.78	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR 3PAR Based Storage - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	1 Terabyte	Fixed Monthly Fee Per Unit		Specific	0	$ 264.02	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 1 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 706.75	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 3 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 1,078.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 10 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 1,562.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond25 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 2,051.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 40 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 2,541.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 100 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 3,605.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 155 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 4,006.75	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 300 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 4,664.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 600 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 5,274.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-1 Resource Unit Price Summary - **Pricing valid through December 31, 2023**.

Resource Unit	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
NetBond 800 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 6,913.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 1000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 7,818.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 2000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 11,786.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 3000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 17,679.75	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 4000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 19,027.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 5000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 20,974.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Enterprise Information Management	n/a	n/a	Quantity	Fixed Fee Per Unit		Specific	0	$ 875,565.65	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Office 365 Network Enabler	n/a	n/a	Quantity	Fixed Monthly Fee Per Unit		Specific	0	$ 184,016.01	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Standard CATA Review	n/a	n/a	Quantity	Fixed Fee Per Unit		Specific	0	$ 56,716.23	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Delta CATA Review	n/a	n/a	Quantity	Fixed Fee Per Unit		Specific	0	$ 28,358.11	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
CATA Strategist	n/a	n/a	Hour	Fixed Fee Per Unit		Cumulative	0	$ 247.84	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
CATA Master	n/a	n/a	Hour	Fixed Fee Per Unit		Cumulative	0	$ 194.90	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
CATA Expert	n/a	n/a	Hour	Fixed Fee Per Unit		Cumulative	0	$ 159.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Oracle on Solaris - Onboarding	n/a	n/a	Server	Fixed Fee Per Unit		Specific	0	$ 120,017.07	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Oracle on Solaris - MRC for Service	n/a	n/a	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 34,323.54	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Oracle on Solaris - MRC per Instance Provisioned	n/a	n/a	Instance	Fixed Monthly Fee Per Unit		Specific	0	$ 35.72	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Public Cloud Provisioning - Onboarding	n/a	n/a	Instance	Fixed Fee Per Unit		Specific	0	$ 5,435.82	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Public Cloud Provisioning - MRC for service	n/a	n/a	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 51,913.91	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Public Cloud Provisioning - MRC per instance provisioned	n/a	n/a	Instance	Fixed Monthly Fee Per Unit		Specific	0	$ 35.72	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

*Schedule 4.3 Reference includes the Section reference for the specific requirements for this particular Resource Unit but it still includes all general requirements applicable to such Resource Unit in the higher levels of the obligations hierarchy as described in Schedule 4.3. For example, the Resource Unit for Desktop - Standard Workstation includes not only the responsibilities as stated in Section 4.5 of the End-User Services Section of Schedule 4.3, but also the responsibilities in Sections 4.1 through 4.3 of the End-User Services Section, as well as the responsibilities and requirements in Section 1 of Schedule 4.3.
**Baseline volume is undetermined at this time
*** The mainframe RU unit volumes are based on the R24 CPUs
****With the exception of 2.3.1.4 and 2.3.1.5, and their respective requirements

Exhibit 16.1-1a – Fees Sample Calculation

Contents

1. Overview 3

2. Non-Bundled Resource Units Calculation 3

3. Bundled Resource Units Calculation....3

4. Third Party Agreements Fees Calculation....5

4.1. Third Party Negotiation – Large....6

4.2. Third Party Negotiation – Small....6

4.3. Third Party Transaction....6

5. Virtual Phone – Microsoft (MS) Teams Phone Advanced Features Resource Account Calculation....9

1. OVERVIEW

Schedule 16.1-1a – Fees Sample Calculations, describes the calculation steps for determining the applicable Resource Unit Fee for Resource Units where banding applies.

2. NON-BUNDLED RESOURCE UNITS CALCULATION

For Resources Units in Exhibit 16.1-1 without a 'bundle' designation (e.g., B1 or B2), the applicable Resource Unit Fee band is determined based on the County's actual volume of consumption for such Resource Unit.

Sample Calculation Data:

Resource Unit (RU): Voice Single Line

Sample Actual Monthly Volume: 3,700

1. Given that the Baseline Volume (per Contract Year) for Voice Single Line per Exhibit 16.1-1 is 39648, the Monthly Baseline volume is 3304.

   Voice Single Line Baseline Volumes (per Contract Year) ÷ 12

   39,648 ÷ 12 = 3,304

2. Given that the Monthly Baseline Volume for Voice Single Line is 3304, the monthly volume thresholds for the various bands are as follows:

   90-110% Threshold for Voice Jack - Single-Line = 3,634 (110% x 3,304)

   110-120% Threshold for Voice Jack - Single-Line = 3,965 (120% x 3,304)

   120-130% Threshold for Voice Jack - Single-Line = 4295 (130% x 3,304)

3. Given that the Sample Actual Monthly Volume is 3700, the 110-120% band should be used to calculate monthly charge for Voice Single Line.

   110-120% Band RU Fee = $2.00 (for purposes of this example only)

   Actual Monthly Volume = 3,700

   Calculation = $2.00 x 3,700

   Sample Monthly Service Fee = $7,400

3. BUNDLED RESOURCE UNITS CALCULATION

For Resources Units in Exhibit 16.1-1 with a 'bundle' designation (e.g. B1 or B2), the applicable Resource Unit Fee band is determined based on the aggregate Actual Monthly volume of all Resource Units within the bundle.

Example 1: In this example, the Actual Monthly volume for the bundle falls within the 90-110% band and therefore all Resource Units within the bundle will use the 90-110% band RU Fee.

Sample Calculation Data:

Resource Unit (RU): Desktop – Standard Workstation

Bundle Designation: B1

Sample Actual Monthly Volume for Desktop – Standard Workstation: 8,000

Sample Actual Monthly Volume for B1: 16,000

a) Given that the Baseline Volume (per Contract Year) for bundle 'B1' per Exhibit 16.1-1 is 179388, the Monthly Baseline volume is 14949.

B1 Baseline Volumes (per Contract Year) ÷ 12

179,388 ÷ 12 = 14,949

b) Given that the Monthly Baseline Volume for bundle 'B1' is 14949, the monthly volume thresholds for the various bands are as follows:

90-110% Threshold for B1= 16,444 (110% x 14,949)

110-120% Threshold for B1= 17,939 (120% x 14,949)

120-130% Threshold for B1= 19,434 (130% x 14,949)

c) Given that the Sample Actual Monthly Volume for bundle 'B1' is 16000, the 90-110% band should be used to calculate monthly charge for Desktop – Standard Workstation and all other Resource Units within the bundle.

90-110% Band RU Fee = $2.00 (for purposes of this example only)

Actual Monthly Volume = 8,000

Calculation = $2.00 x 8,000

Sample Monthly Service Fee = $16,000

Example 2: In this example, the Actual Monthly volume for the bundle falls outside the 90-110% band and therefore the banding in Exhibit 16.1-1 should be applied individually to each Resource Unit within the bundle.

Sample Calculation Data:

Resource Unit (RU): Desktop – Standard Workstation

Bundle Designation: B1

Sample Actual Monthly Volume for Desktop – Standard Workstation: 8,000

Sample Actual Monthly Volume for B1: 17,000

a) Given that the Baseline Volume (per Contract Year) for bundle 'B1' per Exhibit 16.1-1 is 179388, the Monthly Baseline volume is 14949.

B1 Baseline Volumes (per Contract Year) ÷ 12

179,388 ÷ 12 = 14,949

b) Given that the Monthly Baseline Volume for bundle 'B1' is 14949, the monthly volume thresholds for the various bands are as follows:

90-110% Threshold for B1= 16,444 (110% x 14,949)

110-120% Threshold for B1= 17,939 (120% x 14,949)

120-130% Threshold for B1= 19,434 (130% x 14,949)

c) Given that the Sample Actual Monthly Volume for bundle 'B1' is 17000 falls outside of the 90-110% band, the banding for Desktop – Standard Workstation in Exhibit 16.1-1 applies instead of the banding for B1.

d) Given that the Baseline Volume (per Contract Year) for Desktop –Standard Workstation per Exhibit 16.1-1 is 112776, the Monthly Baseline volume is 9398.

Desktop – Standard Workstation Baseline Volumes (per Contract Year) ÷ 12

112,776 ÷ 12 = 9,398

e) Given that the Monthly Baseline Volume for Desktop –Standard Workstation is 9398, the monthly volume thresholds for the various bands are as follows:

70-80% Threshold for Desktop – Standard Workstation = 7,518 (80% x 9,398)

80-90% Threshold for Desktop – Standard Workstation = 8,458 (90% x 9,398)

90-110% Threshold for Desktop – Standard Workstation = 10,338 (110% x 9,398)

f) Given that the Sample Actual Monthly Volume for Desktop – Standard Workstation is 8000, the 80-90% band should be used to calculate monthly charge for Desktop – Standard Workstation.

80-90% Band RU Fee = $1.00 (for purposes of this example only)

Actual Monthly Volume = 8,000

Calculation = $1.00 x 8,000

Sample Monthly Service Fee = $8,000

4. THIRD PARTY AGREEMENTS FEES CALCULATION

Below are sample calculations for the three-tiered level pricing for Third-Party Agreements.

4.1. Third Party Negotiation – Large

Example 1: County requests Contractor to contract and purchase software licenses and implementation labor from company AAA. Company AAA is not a third-party vendor currently contracted by Contractor in support of the Services. The vendor price of the software is $300,000 plus $50,000 for the first year of software maintenance. The vendor price for implementation labor is $200,000.

a) Given that company AAA is not a Third-Party vendor currently contracted by Contractor in support of Services, and the transaction amount is in excess $500,000, the Third Party Negotiation – Large Resource Unit Fee applies.

   Third Party Negotiation – Large = $10,000

b) Additionally, the Third Party Transaction Resource Unit Fee of 5% applies to the transaction amount.

   ($300,000 + $50,000 + $200,000) x 5% = $27,500

Total fees are $37,500.

4.2. Third Party Negotiation – Small

Example 1: County requests Contractor to contract and purchase software licenses from company BBB. Company BBB is not a Third-Party vendor currently contracted by Contractor in support of the Services. The vendor price of the software is $80,000 plus $20,000 for the first year of software maintenance.

a) Given that company BBB is not a Third-Party vendor currently contracted by Contractor in support of Services, and the transaction amount is less than $500,000, the Third Party Negotiation – Small Resource Unit Fee applies.

   Third Party Negotiation – Small = $5,000

b) Additionally, the Third Party Transaction Resource Unit Fee of 5% applies to the transaction amount.

   ($80,000 + $20,000) x 5% = $5,000

Total fees are $10,000.

4.3. Third Party Transaction

Example 1 (License Maintenance Renewal): Per County request, Contractor procures software maintenance renewal from vendor AAA. Vendor AAA is a Third-Party vendor that has not contracted with Contractor before. Contractor issues a Purchase Order (PO) in the amount of $20,000 for the software maintenance renewal.

Given that Contractor negotiated a new agreement with Vendor AAA, the Third Party Negotiation – Small and Third Party Transaction Resource Unit Fees apply.

Formula:	Third Party Negotiation – Small + (5% x PO amount)
Fee Calculation:	$5,000 + (5% x $20,000) = $6,000
	Note: The Third Party Transaction Fee of 5% is applied to each invoice received from Vendor AAA.

Example 2 (Perpetual License Purchase): Per County request, Contractor procures perpetual licenses from vendor BBB. Vendor BBB is a Third-Party vendor already contracted by Contractor in support of the Services. Contractor issues a PO in the amount of $1.1M for the perpetual licenses.

Given that Contractor did not negotiate a new agreement with Vendor BBB, only the Third Party Transaction Resource Unit Fee applies.

Formula:	5% x PO amount
Fee Calculation:	5% x $1.1M = $55,000
Actual Fee:	$50,000 (due to fee maximum of $50,000)
	Note: The Third Party Transaction Fee of 5% is applied to each invoice received from Vendor BBB up to the maximum amount of $50,000.

Example 3 (Hardware): Per County request, Contractor procures one large scanner not available in the Optional Item Catalog or as a Resource Unit. The scanner is purchased through a Third-Party vendor already contracted by Contractor in support of the Services. Contractor issues a PO in the amount of $1,000 for the scanner.

Given that Contractor did not negotiate a new agreement with Third-Party vendor, only the Third Party Transaction Resource Unit Fee applies.

Formula:	5% x PO amount
Fee Calculation:	5% x $1,000 = $50
Actual Fee:	$100 (due to fee minimum of $100)
	Note: The Third Party Transaction Fee of $100 is applied to the invoice.

Example 4 (Labor Statement of Work): Per County request, Contractor contracts with vendor DDD for a project. Vendor DDD has not contracted with Contractor before. Contractor issues a PO in the amount of $750,000 based on a Statement of Work.

Given that Contractor negotiated a new agreement with Vendor DDD, the Third Party Negotiation – Large and Third Party Transaction Resource Unit Fees apply.

Formula: Third Party Negotiation – Small + (5% x PO amount)

Fee Calculation: $10,000 + (5% x $750,000) = $47,500

Note: The Third Party Transaction Fee of 5% is applied to each invoice received from Vendor DDD.

Example 5 (Labor Statement of Work Change Request): Per County request, Contractor issues a Change Request to Vendor DDD (see Example 4 above) in the amount of $500,000. The PO total is now $1.2M.

Formula: (5% x PO amount up to $1M) +
(4% x PO amount between $1M - $10M)

Fee Calculation: (5% x $1M) + (4% x $250,000) = $60,000

Note: The applicable Third Party Transaction Fee Tier is applied to each invoice received from Vendor DDD. The 5% fee is applied until aggregate amount of all invoices from the vendor reaches the $1M threshold, then the 4% fee is applied to any further invoice.

Example 6 (Labor Statement of Work): Per County request, Contractor contracts with vendor EEE for a project. Vendor EEE is a Third-Party vendor already contracted by Contractor in support of the Services. Contractor issues a PO in the amount of $3M based on a Statement of Work.

Given that Contractor did not negotiate a new agreement with Vendor EEE, only the Third Party Transaction Resource Unit Fee applies.

Formula: 4% x PO amount

Fee Calculation: 4% x $3M = $120,000
Note: The Third Party Transaction Fee Tier of 4% is applied to each invoice received from Vendor EEE.

Example 7 (SaaS License Subscription): Per County request, Contractor procures licenses from vendor FFF through a three-year subscription agreement with a Total Contract Value of $1.8M. Vendor FFF is a Third-Party vendor already contracted by Contractor in support of the Services. Contractor issues a PO in the amount of $600K for the 1st year of subscription.

Given that Contractor did not negotiate a new agreement with Vendor FFF, only the Third Party Transaction Resource Unit Fee applies.

Formula: 4% x PO amount
Fee Calculation: 4% x $600,000 = $24,000 for the 1st year
4% x $600,000 = $24,000 for the 2nd year
4% x $600,000 = $24,000 for the 3rd year
Note: The Third Party Transaction Fee Tier of 4% is applied to each invoice received from Vendor FFF.

5. VIRTUAL PHONE – MICROSOFT (MS) TEAMS PHONE ADVANCED FEATURES RESOURCE ACCOUNT CALCULATION

Below are sample calculations for the Resource Account Licenses associated with Virtual Phone – Microsoft (MS) Teams Phone Advanced Feature RU.

Example 1: County department has one (1) call flow with two (2) auto-attendants and one (1) call queue.

In addition to being billed the Virtual Phone – Microsoft (MS) Teams Phone Advanced features monthly Resource unit (RU) fee, the County department shall be billed for three (3) Resource Account licenses monthly via the Catalog RU and the applicable number of Virtual Phone – MS Teams Phone RU associated with the call flow.

Example 2: County department has two (2) call flows set-up with ten (10) auto-attendants and five (5) call queues. The County department will be billed as follows:

2 x Virtual Phone – MS Teams Phone Advanced Features monthly RU fee

Thirty (30) Resource Account licenses monthly RU fee

Applicable number of Virtual Phone – MS Teams Phone RU associated with the call flow

END OF SCHEDULE

Exhibit 16.1-1 – Appendix 1 New Site Install Variable Components

Exhibit 16.1-1 Appendix 1 New Site Install Variable Components

Mfg	Description	MDF						IDF						Backbone						Drop					
		Type 1	Type 2	Type 3	Type 4	Type 5	Type 6	Type 1	Type 2	Type 3	Type 4	Type 5	Type 6	Type 1	Type 2	Type 3	Type 4	Type 5	Type 6	Type 1	Type 2	Type 3	Type 4	Type 5	Type 6
		1,000+	501-999	250-500	50-249	11-49	0-10	1,000+	501-999	250-500	50-249	11-49	0-10	1,000+	501-999	250-500	50-249	11-49	0-10	1,000+	501-999	250-500	50-249	11-49	0-10
CPI	2 post 19" x 7' open bay rack	4	3	3	2	2	1	2	2	2	1	1	1												
CPI	Rack to runway plate 12"	4	3	3	2	2	1	2	2	2	1	1	1												
CPI	12"W x 10'L ladder rack	5	5	5	5	5	3	5	5	5	3	3	3												
CPI	Wall angle bracket 12"	4	4	4	4	4	3	4	4	4	3	3	3												
CPI	Triangle wall bracket 12"	6	6	6	6	6	5	6	6	6	5	5	5												
CPI	Butt-splice kit 1-1/2 x 3/8	4	4	4	4	4	2	4	4	4	2	2	2												
CPI	Junction-splice kit 1-1/2 x 3/8	7	7	7	7	7	5	7	7	7	5	5	5												
CPI	Protective end caps	3	3	3	3	3	2	3	3	3	2	2	2												
Panduit	Vertical wire manager 45RU	5	4	4	3	3	2	3	3	3	2	2	2												
OPEN	THNN-6-STR-GRN	50	45	45	40	40	35	40	40	40	35	35	35												
Burndy	#6 long barrel 2 hole ground lug	20	18	18	16	16	12	16	16	16	12	12	12												
Corning	MIC 24F OM3 armored plenum													500	500	500	500	500	500						
Corning	MIC 24F SM armored plenum																								
Corning	MIC 12F OM3 armored plenum																								
Corning	MIC 12F SM armored plenum																								
Corning	LC connector OM3 unicam													48	48	48	48	48	48						
Corning	LC connector SM unicam																								
Corning	Adapter panel 12F LC OM3													4	4	4	4	4	4						
Corning	Adapter panel 12F LC SM																								
Corning	Rack mount fiber enclosure 1U													1	1	1	1	1	1						
Corning	Rack mount fiber enclosure 2U	1	1	1	1	1	1																		
Endot	1.25" innerduct plenum white													500	500	500	500	500	500						
Sup. Essex	50 pair level 3 cable plenum													500	500	500	500	500	500						
Sup. Essex	100 pair level 3 cable plenum																								
Ortronics	110 block w/ clips Cat5e 300pr													2	2	2	2	2	2						
Ortronics	110 jumper trough w/legs													8	8	8	8	8	8						
Ortronics	24port Cat5e patch panel	1	1	1	1	1	1							1	1	1	1	1	1						
Berk-Tek	Cat5e plenum cable blue																			250	250	250	250	250	250
Ortronics	Cat5e Keystone RJ45 blue																			1	1	1	1	1	1
AMP	3 port furniture plate black																			1	1	1	1	1	1
AMP	48port Cat5e patch panel																			0.021	0.021	0.021	0.021	0.021	0.021
AMP	Blank insert black																			2	2	2	2	2	2
Allen Tel	1' Cat5e patch cord white																			1	1	1	1	1	1
Allen Tel	14' Cat5e patch cord white																			1	1	1	1	1	1
Generic	2" j-hook w/clip																			5	5	5	5	5	5
Generic	20' hang wire straight																			5	5	5	5	5	5
Misc	Auto-Cad (drawings)																			1	1	1	1	1	1
Misc	Consumables																			1	1	1	1	1	1

Exhibit 16.1-2 – Resource Unit Price Decomposition

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
Contract and Acquisition Management Services	***Schedule 4.3 Section 2.3	Month	Fixed Monthly Fee Per Unit		$ 211,810.14		
				Service Desk Services		$ 5,688.40	Represents the portion of Contract Management labor attributable to providing Service Desk Services.
				End User Services		$ 34,928.89	Represents the portion of Contract Management labor attributable to providing End User Services.
				Network Services		$ 68,275.17	Represents the portion of Contract Management labor attributable to providing Network Services.
				Data Center Services		$ 30,730.18	Represents the portion of Contract Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 24,808.82	Represents the portion of Contract Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 47,378.68	Represents the portion of Contract Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 211,810.14	Represents the labor to support Contract and Acquisition Management Services as defined in Schedule 4.3, Section 2.3.
Integrated Asset Management Services	Schedule 4.3 - Section 2.4	Month	Fixed Monthly Fee Per Unit		$ 112,804.78		
				Service Desk Services		$ 3,029.50	Represents the portion of Asset Management labor attributable to providing Service Desk Services.
				End User Services		$ 18,602.25	Represents the portion of Asset Management labor attributable to providing End User Services.
				Network Services		$ 36,361.65	Represents the portion of Asset Management labor attributable to providing Network Services.
				Data Center Services		$ 16,366.12	Represents the portion of Asset Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 13,212.56	Represents the portion of Asset Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 25,232.70	Represents the portion of Asset Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 112,804.78	Represents the labor to support Integrated Asset Management Services as defined in Schedule 4.3, Section 2.4.
Billing Management Services	Schedule 4.3 - Section 2.5	Month	Fixed Monthly Fee Per Unit		$ 41,890.53		
				Service Desk Services		$ 1,125.02	Represents the portion of Billing Management labor attributable to providing Service Desk Services.
				End User Services		$ 6,908.02	Represents the portion of Billing Management labor attributable to providing End User Services.
				Network Services		$ 13,503.05	Represents the portion of Billing Management labor attributable to providing Network Services.
				Data Center Services		$ 6,077.63	Represents the portion of Billing Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 4,906.54	Represents the portion of Billing Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 9,370.27	Represents the portion of Billing Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 41,890.53	Represents the labor to support Billing Management Services as defined in Schedule 4.3, Section 2.5.
Security Management Services	Schedule 4.3 - Section 2.6	Month	Fixed Monthly Fee Per Unit		$ 240,747.14		
				Service Desk Services		$ 7,246.31	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Service Desk Services.
				End User Services		$ 44,495.03	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of End User Services.
				Network Services		$ 57,901.58	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Network Services.
				Data Center Services		$ 39,146.40	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Data Center Services.
				Application Maintenance & Operations Services		$ 31,603.34	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Applications Maintenance & Operations Services.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Application Development Services		$ 60,354.50	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Application Development Services.
				Hardware		$ -	N/A
				Software		$ 2,657.88	Represents Software tools to support the County Environment.
				Labor		$ 238,089.26	Represents the labor to support Security Management Services as defined in Schedule 4.3, Section 2.6.
Malware Protection	Schedule 4.3 Section 2.6	Month	Fixed Monthly Per Unit		$ 5,062.50		
				Hardware			
				Software		$ 2,812.50	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance			N/A
				Software Support		$ 2,250.00	Third-Party vendor and ITO support, including implementation of County required changes and modifications after the initial integration.
Secure Internet Access	Schedule 4.3 Section 2.6	Month	Fixed Monthly Per Unit		$ 27,100.00		
				Hardware			N/A
				Software		$ 17,500.00	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance			N/A
				Software Support		$ 9,600.00	Third-Party vendor and ITO support, including implementation of County required changes and modifications after the initial integration.
Multi-Factor Authentication Service	Schedule 4.3 Section 2.6	Month	Fixed Monthly Per Unit		$ 42,152.00		
				Hardware		$ -	
				Operating System License		$ -	
				Other Software License		$ 22,500.00	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	
				Software Maintenance		$ 19,652.00	Represents costs associated with software maintenance along with the labor and resources for support by vendor and Contractor.
Service Delivery Management Services	Schedule 4.3 - Section 2.7	Month	Fixed Monthly Fee Per Unit		$ 197,508.06		
				Service Desk Services		$ 6,368.85	Represents the portion of Service Delivery Management labor attributable to providing Service Desk Services.
				End User Services		$ 39,107.13	Represents the portion of Service Delivery Management labor attributable to providing End User Services.
				Network Services		$ 36,803.24	Represents the portion of Service Delivery Management labor attributable to providing Network Services.
				Data Center Services		$ 34,406.17	Represents the portion of Service Delivery Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 27,776.49	Represents the portion of Service Delivery Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 53,046.18	Represents the portion of Service Delivery Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 197,508.06	Represents the labor to support SDM Services as defined in Schedule 4.3, Section 2.7.
Project Management Services	Schedule 4.3 - Section 2.9	Month	Fixed Monthly Fee Per Unit		$ 133,967.13		
				Service Desk Services		$ 3,597.84	Represents the portion of Project Management labor attributable to providing Service Desk Services.
				End User Services		$ 22,092.06	Represents the portion of Project Management labor attributable to providing End User Services.
				Network Services		$ 43,183.15	Represents the portion of Project Management labor attributable to providing Network Services.
				Data Center Services		$ 19,436.43	Represents the portion of Project Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 15,691.26	Represents the portion of Project Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 29,966.39	Represents the portion of Project Management labor attributable to providing Application Development Services.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 133,967.13	Represents the labor to support Project Management Services as defined in Schedule 4.3, Section 2.9.
Integration and Testing Services	Schedule 4.3 - Section 2.10	Month	Fixed Monthly Fee Per Unit		$ 36,346.87		
				Service Desk Services		$ 976.14	Represents the portion of Integration and Testing labor attributable to providing Service Desk Services.
				End User Services		$ 5,993.84	Represents the portion of Integration and Testing labor attributable to providing End User Services.
				Network Services		$ 11,716.10	Represents the portion of Integration and Testing labor attributable to providing Network Services.
				Data Center Services		$ 5,273.33	Represents the portion of Integration and Testing labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 4,257.22	Represents the portion of Integration and Testing labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 8,130.24	Represents the portion of Integration and Testing labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 36,346.87	Represents the labor to support Integrated and Testing Services as defined in Schedule 4.3, Section 2.10.
Incident Management Services	Schedule 4.3 - Section 2.11	Month	Fixed Monthly Fee Per Unit		$ 3,316.47		
				Service Desk Services		$ 89.07	Represents the portion of Incident Management labor attributable to providing Service Desk Services.
				End User Services		$ 546.91	Represents the portion of Incident Management labor attributable to providing End User Services.
				Network Services		$ 1,069.04	Represents the portion of Incident Management labor attributable to providing Network Services.
				Data Center Services		$ 481.17	Represents the portion of Incident Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 388.45	Represents the portion of Incident Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 741.84	Represents the portion of Incident Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 3,316.47	Represents the labor to support Incident Management Services as defined in Schedule 4.3, Section 2.11.
Problem Management Services	Schedule 4.3 - Section 2.12	Month	Fixed Monthly Fee Per Unit		$ 3,316.47		
				Service Desk Services		$ 89.07	Represents the portion of Problem Management labor attributable to providing Service Desk Services.
				End User Services		$ 546.91	Represents the portion of Problem Management labor attributable to providing End User Services.
				Network Services		$ 1,069.04	Represents the portion of Problem Management labor attributable to providing Network Services.
				Data Center Services		$ 481.17	Represents the portion of Problem Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 388.45	Represents the portion of Problem Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 741.84	Represents the portion of Problem Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 3,316.47	Represents the labor to support Problem Management Services as defined in Schedule 4.3, Section 2.12.
Change Management Services	Schedule 4.3 - Section 2.13	Month	Fixed Monthly Fee Per Unit		$ 9,310.92		
				Service Desk Services		$ 250.06	Represents the portion of Change Management labor attributable to providing Service Desk Services.
				End User Services		$ 1,535.43	Represents the portion of Change Management labor attributable to providing End User Services.
				Network Services		$ 3,001.30	Represents the portion of Change Management labor attributable to providing Network Services.
				Data Center Services		$ 1,350.86	Represents the portion of Change Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 1,090.57	Represents the portion of Change Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 2,082.71	Represents the portion of Change Management labor attributable to providing Application Development Services.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 9,310.92	Represents the labor to support Change Management Services as defined in Schedule 4.3, Section 2.13.
Release Management Services	Schedule 4.3 - Section 2.14	Month	Fixed Monthly Fee Per Unit		$ 10,477.58		
				Service Desk Services		$ 281.39	Represents the portion of Release Management labor attributable to providing Service Desk Services.
				End User Services		$ 1,727.82	Represents the portion of Release Management labor attributable to providing End User Services.
				Network Services		$ 3,377.36	Represents the portion of Release Management labor attributable to providing Network Services.
				Data Center Services		$ 1,520.13	Represents the portion of Release Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 1,227.21	Represents the portion of Release Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 2,343.67	Represents the portion of Release Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 10,477.58	Represents the labor to support Release Management Services as defined in Schedule 4.3, Section 2.14.
Configuration Management	Schedule 4.3 - Section 2.15	Month	Fixed Monthly Fee Per Unit		$ 18,074.33		
				Service Desk Services		$ 485.41	Represents the portion of Configuration Management labor attributable to providing Service Desk Services.
				End User Services		$ 2,980.58	Represents the portion of Configuration Management labor attributable to providing End User Services.
				Network Services		$ 5,826.10	Represents the portion of Configuration Management labor attributable to providing Network Services.
				Data Center Services		$ 2,622.29	Represents the portion of Configuration Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 2,117.00	Represents the portion of Configuration Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 4,042.95	Represents the portion of Configuration Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 18,074.33	Represents the labor to support Configuration Management Services as defined in Schedule 4.3, Section 2.15.
Capacity Planning and Performance Management Services	Schedule 4.3 - Section 2.16	Month	Fixed Monthly Fee Per Unit		$ 17,497.78		
				Service Desk Services		$ 469.92	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Service Desk Services.
				End User Services		$ 2,885.50	Represents the portion of Capacity Planning and Performance Management labor attributable to providing End User Services.
				Network Services		$ 5,640.26	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Network Services.
				Data Center Services		$ 2,538.64	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 2,049.47	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 3,913.99	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 17,497.78	Represents the labor to support Capacity Planning and Performance Management Services as defined in Schedule 4.3, Section 2.16.
Disaster Recovery Management Services	Schedule 4.3 - Section 2.17	Month	Fixed Monthly Fee Per Unit		$ 208,849.96		
				Service Desk Services		$ 104.42	Represents the labor required to manage, update and test the Disaster Recovery Plan for Service Desk Services.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				End User Services		$ 208.85	Represents the labor required to manage and update Disaster Recovery Plan documents for End User Services. This includes providing input to County Business Continuity Plans and supporting testing as needed.
				Network Services		$ 41,769.99	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Network Disaster Recovery Services.
				Data Center Services		$ 156,324.19	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Data Center Disaster Recovery Services.
				Application Maintenance & Operations Services		$ 10,442.50	Represents the labor required to manage, update and test the Technical Recovery Plans for individual Applications, within the scope of the Data Center Disaster Recovery Plan.
				Application Development Services		$ -	N/A
				Hardware		$ 124,535.16	Represents the servers routers, switches, and storage equipment required to support DR environment.
				Software		$ 34,298.94	Represents the software costs associated with DR hardware used to support the DR environment.
				Labor		$ 50,015.86	Represents the labor to support Disaster Recovery Management Services as defined in Schedule 4.3, Section 2.17.
Identity Access Management Services	Schedule 4.3 - Section 2.18	Month	Fixed Monthly Fee Per Unit		$ 147,777.10		
				Service Desk Services		$ 3,968.72	Represents the portion of Identity Access Management labor attributable to providing Service Desk Services.
				End User Services		$ 24,369.42	Represents the portion of Identity Access Management labor attributable to providing End User Services.
				Network Services		$ 47,634.68	Represents the portion of Identity Access Management labor attributable to providing Network Services.
				Data Center Services		$ 21,440.03	Represents the portion of Identity Access Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 17,308.79	Represents the portion of Identity Access Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 33,055.47	Represents the portion of Identity Access Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ 23,731.41	Includes Symantec PKI Maintenance and Tools for IDAM resources to support the County environment.
				Labor		$ 124,045.69	Represents the labor to support Identity Access Management Services as defined in Schedule 4.3, Section 2.18.
Reporting Management Services	Schedule 4.3 - Section 2.19	Month	Fixed Monthly Fee Per Unit		$ 73,993.82		
				Service Desk Services		$ 1,987.19	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Service Desk Services.
				End User Services		$ 12,202.07	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of End User Services.
				Network Services		$ 23,851.27	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Network Services.
				Data Center Services		$ 10,735.29	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Data Center Services.
				Application Maintenance & Operations Services		$ 8,666.72	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Applications Maintenance & Operations Services.
				Application Development Services		$ 16,551.28	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 73,993.82	Represents the labor to support Reporting Management Services as defined in Schedule 4.3, Section 2.19.
Domain Name Management Services	Schedule 4.3 - Section 2.20	Month	Fixed Monthly Fee Per Unit		$ 1,523.67		
				Service Desk Services		$ -	N/A
				End User Services		$ -	N/A
				Network Services		$ 1,523.67	Represents the portion of Domain Name Management labor attributable to providing Network Services.
				Data Center Services		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Application Maintenance & Operations Services		$ -	N/A
				Application Development Services		$ -	N/A
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 1,523.67	Represents the labor to support Domain Name Management Services as defined in Schedule 4.3, Section 2.20.
Business Analyst Services	Schedule 4.3 - Section 2.21	Month	Fixed Monthly Fee Per Unit		$ 79,296.61		
				Service Desk Services		$ 2,985.45	Represents the portion of Business Analyst Services labor attributable to providing Service Desk Services.
				End User Services		$ 18,331.81	Represents the portion of Business Analyst Services labor attributable to providing End User Services.
				Network Services		$ 3,964.83	Represents the portion of Business Analyst Services labor attributable to providing Network Services.
				Data Center Services		$ 16,128.19	Represents the portion of Business Analyst Services labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 13,020.47	Represents the portion of Business Analyst Services labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 24,865.86	Represents the portion of Business Analyst Services labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 79,296.61	Represents the labor to support Business Analyst Services as defined in Schedule 4.3, Section 2.21.
Chief Technical Architect Services	Schedule 4.3 - Section 2.22	Month	Fixed Monthly Fee Per Unit		$ 18,188.23		
				Service Desk Services		$ 3,031.37	Represents the portion of CTA labor attributable to providing Service Desk Services.
				End User Services		$ 3,031.37	Represents the portion of CTA labor attributable to providing End User Services.
				Network Services		$ 3,031.37	Represents the portion of CTA labor attributable to providing Network Services.
				Data Center Services		$ 3,031.37	Represents the portion of CTA labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 3,031.37	Represents the portion of CTA labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 3,031.37	Represents the portion of CTA labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 18,188.23	Represents the labor to support CTA Services as defined in Schedule 4.3, Section 2.22.
Enterprise Applications Architect Services	Schedule 4.3 - Section 2.23	Month	Fixed Monthly Fee Per Unit		$ 18,188.23		
				Service Desk Services		$ 3,031.37	Represents the portion of EAA labor attributable to providing Service Desk Services.
				End User Services		$ 3,031.37	Represents the portion of EAA labor attributable to providing End User Services.
				Network Services		$ 3,031.37	Represents the portion of EAA labor attributable to providing Network Services.
				Data Center Services		$ 3,031.37	Represents the portion of EAA labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 3,031.37	Represents the portion of EAA labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 3,031.37	Represents the portion of EAA labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 18,188.23	Represents the labor to support EAA Services as defined in Schedule 4.3, Section 2.23.
Innovation Management Services	Schedule 4.3 - Section 2.24	Month	Fixed Monthly Fee Per Unit		$ 20,069.65		
				Service Desk Services		$ 3,344.94	Represents the portion of Innovation Management labor attributable to providing Service Desk Services.
				End User Services		$ 3,344.94	Represents the portion of Innovation Management labor attributable to providing End User Services.
				Network Services		$ 3,344.94	Represents the portion of Innovation Management labor attributable to providing Network Services.
				Data Center Services		$ 3,344.94	Represents the portion of Innovation Management labor attributable to providing Data Center Services.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Application Maintenance & Operations Services		$ 3,344.94	Represents the portion of Innovation Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 3,344.94	Represents the portion of Innovation Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 20,069.65	Represents the labor to support Innovation Management Services as defined in Schedule 4.3, Section 2.24.
Service Desk Services	Section 3.0	Month	Fixed Monthly Fee Per Unit		$ 198,226.81		
				Service Desk Services		$ 5,323.60	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Service Desk Services.
				End User Services		$ 32,688.91	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support End User Services.
				Network Services		$ 63,896.71	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Network Services.
				Data Center Services		$ 28,759.46	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Data Center Services.
				Application Maintenance & Operations Services		$ 23,217.84	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support App Maintenance Services.
				Application Development Services		$ 44,340.29	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support App Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 198,226.81	Represents the labor to support Service Desk Services as defined in Schedule 4.3, Section 2.3.
Duo Hardware Token MFA	Schedule 4.3 - Section 4.5.2	Account	Fixed Monthly Fee Per Unit		$ 5.28		
				Hardware		$ -	N/A
				Software License		$ 2.97	Represents the cost of software license subscription.
				IMARS		$ 2.31	Represents labor costs for IMAR activities, Tier 1 Helpdesk.
Electronic Signature	Schedule 4.3 - Section 4.5.2	Transaction	Fixed Fee Per Unit		$ 1.01		
				Hardware		$ -	N/A
				Hardware (Refresh Labor)		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ -	N/A
				Software Maintenance		$ 0.81	Represents the cost associated to the software maintenance and labor costs.
				IMAR's		$ 0.0074	Represents the cost associated to the IMAR labor.
				Service Desk		$ 0.19	Represents costs associated with Service Desk labor.
Desktop - 3D Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 273.69		
				Hardware		$ 145.06	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 26.90	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 28.71	Represents break-fix services, primarily labor and parts.
				Software License		$ 21.51	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 39.47	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 10.78	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 1.26	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Advanced Engineering Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 210.24		
				Hardware		$ 120.00	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 4 years.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware (Refresh Labor)		$ 18.92	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 20.24	Represents break-fix services, primarily labor and parts.
				Software License		$ 15.13	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 27.74	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 7.64	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.57	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Advanced Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 94.11		
				Hardware		$ 49.88	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 9.25	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 9.87	Represents break-fix services, primarily labor and parts.
				Software License		$ 7.40	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 13.57	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.71	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.43	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Engineering Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 111.13		
				Hardware		$ 64.61	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 10.72	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 7.88	Represents break-fix services, primarily labor and parts.
				Software License		$ 7.47	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 16.31	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.57	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.56	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Gold Engineering Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 295.72		
				Hardware		$ 205.48	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 18.92	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 20.24	Represents break-fix services, primarily labor and parts.
				Software License		$ 15.13	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 27.74	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 7.64	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.57	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Mini Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 64.96		
				Hardware		$ 30.56	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 6.00	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 5.31	Represents break-fix services, primarily labor and parts.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software License		$ 6.05	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 14.53	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.00	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.50	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Small Form Factor with Optical Drive	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 64.96		
				Hardware		$ 30.56	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 6.00	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 5.31	Represents break-fix services, primarily labor and parts.
				Software License		$ 6.05	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 14.53	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.00	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.50	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Standard Workstation	Schedule 4.3 - Section 4.5.3	Quantity	Fixed Monthly Per Unit		$ 64.96		
				Hardware		$ 30.56	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 6.00	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 5.31	Represents break-fix services, primarily labor and parts.
				Software License		$ 6.05	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 14.53	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.00	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.50	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Scanner	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 136.17		
				Hardware		$ 105.13	Represents the costs of acquiring the asset, including feeder consumable kit. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 3.12	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 24.11	Represents break-fix services, primarily labor and parts, including annual preventive maintenance.
				Software License		$ -	N/A
				Software Maintenance		$ -	N/A
				IMAR's		$ 3.81	Represents labor costs for IMAR activities.
Laptop - Engineering	Schedule 4.3 - Section 4.5.3	Device	Fixed monthly fee per unit		$ 165.27		
				Hardware		$ 87.76	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 16.26	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 17.39	Represents break-fix services, primarily labor and parts.
				Software License		$ 12.96	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 23.93	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 6.54	Represents labor costs for IMAR activities.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Desktop Application Directory Maintenance		$ 0.43	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Ruggedized	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 188.33		
				Hardware		$ 120.73	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 11.27	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 10.60	Represents break-fix services, primarily labor and parts.
				Software License		$ 17.30	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 24.11	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.76	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.56	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Standard	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 86.55		
				Hardware		$ 40.41	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 7.91	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 5.33	Represents break-fix services, primarily labor and parts.
				Software License		$ 12.38	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 17.35	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.64	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.52	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Standard LTE	Schedule 4.3 - Section 4.5.3	Device	Fixed monthly fee per unit		$109.10		
				Hardware		$ 57.93	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 10.74	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 11.47	Represents break-fix services, primarily labor and parts.
				Software License		$ 8.56	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 15.80	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 4.32	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.28	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Ultra Portable	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 93.86		
				Hardware		$ 45.20	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 8.07	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 7.63	Represents break-fix services, primarily labor and parts.
				Software License		$ 12.45	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 17.25	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.69	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.56	Represents the labor associated with maintaining the Desktop Application Directory.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
Laptop - Ultra Portable 2in1	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 106.48		
				Hardware		$ 51.27	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 9.21	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 8.66	Represents break-fix services, primarily labor and parts.
				Software License		$ 14.13	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 19.57	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.07	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.56	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Convertible	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 95.28		
				Hardware		$ 50.70	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 7.30	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 6.99	Represents break-fix services, primarily labor and parts.
				Software License		$ 11.41	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 15.94	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.43	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.51	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Ruggedized	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 209.83		
				Hardware		$ 139.68	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 11.44	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 11.00	Represents break-fix services, primarily labor and parts.
				Software License		$ 17.95	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 25.38	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.81	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.57	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Surface Pro	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 106.92		
				Hardware		$ 56.89	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 8.03	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 7.85	Represents break-fix services, primarily labor and parts.
				Software License		$ 12.80	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 18.10	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.68	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.57	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Surface Pro LTE	Schedule 4.3 - Section 4.5.3	Device	Fixed monthly fee per unit		$138.02		

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware		$ 73.28	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 13.58	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 14.52	Represents break-fix services, primarily labor and parts.
				Software License		$ 10.82	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 19.98	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 5.47	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.37	Represents the labor associated with maintaining the Desktop Application Directory.
County Retained Device	Schedule 4.3 - Section 4.7.3	Device	Fixed Monthly Per Unit		$ 103.09		
				Software License		$ 12.34	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 17.45	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 72.75	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.55	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - DCSS	Schedule 4.3 - Section 4.7.3	Device	Fixed Monthly Per Unit		$ 36.23		
				Hardware (Refresh Labor)		$ 3.36	Represents the labor for providing support for refresh tasks, on a 4-year cycle.
				Hardware Maintenance		$ 5.81	Represents break-fix services, primarily labor and parts.
				Software License		$ 5.43	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 10.44	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 8.74	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.53	Represents the labor associated with maintaining the Desktop Application Directory.
				Printer Maintenance		$ 1.91	Represents Level 2 printer support.
Laptop - DCSS	Schedule 4.3 - Section 4.7.3	Device	Fixed Monthly Per Unit		$ 44.31		
				Hardware (Refresh Labor)		$ 3.36	Represents the labor for providing support for refresh tasks, on a 3-year cycle.
				Hardware Maintenance		$ 7.23	Represents break-fix services, primarily labor and parts.
				Software License		$ 6.65	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 13.12	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 10.89	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.68	Represents the labor associated with maintaining the Desktop Application Directory.
				Printer Maintenance		$ 2.38	Represents Level 2 printer support.
Mobile Devices Support Services - Intune	Section 4.8	Device	Fixed Monthly Fee Per Unit		$ 7.51		
				Software License		$ -	Represents the costs of AirWatch software licenses upgrades/refresh. The aggregated cost is apportioned over the volume of Mobile Devices.
				Software Maintenance		$ 1.94	Represents costs associated with the labor and resources for Level 2 support and centralized hosting costs for Mobile Services applications.
				IMAR's		$ 5.57	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
Printer - Color Network Workgroup - Large Format (CNWP-LF)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 165.77		
				Hardware		$ 86.99	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 3.32	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 72.39	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 3.07	Represents labor costs for IMAR activities.
Printer - Color Network Workgroup - Standard Format (CNWP)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 67.57		
				Hardware		$ 40.87	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 1.01	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 23.33	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 2.36	Represents labor costs for IMAR activities.
Printer - Monochrome Network Workgroup - Standard Format (MNWP)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 60.49		
				Hardware		$ 36.37	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 1.21	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 21.81	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 1.10	Represents labor costs for IMAR activities.
Printer - Monochrome Network Workgroup - Large Format (MNWP-LF)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 97.43		
				Hardware		$ 67.29	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 1.95	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 26.63	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 1.56	Represents labor costs for IMAR activities.
Printer - Monochrome Network High Volume - Large Format (MNWP-LF-H)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 158.88		
				Hardware		$ 101.17	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 2.35	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 48.77	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 6.59	Represents labor costs for IMAR activities.
Electronic File Sharing Services	Schedule 4.3 -- Section 4.12	User	Fixed Monthly Fee Per Unit		$ 81.25		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 37.26	Represents the license cost attributable to providing this service.
				Labor		$ 43.99	Represents the labor cost (e.g. Service Desk, IMAR, platform administration) to support the solution.
A/V Conference Room - Large	Schedule 4.3 - Section 4.13	Install	Fixed Fee Per Unit		$ 64,563.91		
				Hardware		$ 53,588.05	Represents the costs to acquire the Hardware
				Software		$ -	
				Labor		$ 10,975.86	Represents the costs to perform the labor for install and ongoing support

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
A/V Conference Room - Medium	Schedule 4.3 - Section 4.13	Install	Fixed Fee Per Unit		$ 34,671.93		
				Hardware		$ 28,777.70	Represents the costs to acquire the Hardware
				Software		$ -	
				Labor		$ 5,894.23	Represents the costs to perform the labor for install and ongoing support
A/V Conference Room - Small	Schedule 4.3 - Section 4.13	Install	Fixed Fee Per Unit		$ 25,004.76		
				Hardware		$ 20,753.95	Represents the costs to acquire the Hardware
				Software		$ -	
				Labor		$ 4,250.81	Represents the costs to perform the labor for install and ongoing support
Digital Signage Services	Schedule 4.3 - Section 4.14	Subscription	Fixed Monthly Fee Per Unit		$ 68.37		
				Hardware		$ 40.00	Represents the third party costs associated with original configuration and monthly subscription payments for a agreed upon term.
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ -	N/A
				Labor		$ 28.37	Represents costs associated with various with initial installation, help desk, and break/fix labor and support.
Survey Solution Support Services	Schedule 4.3 - Section 4.16	Administrator	Fixed Monthly Fee Per Unit		$ 48.94		
				Hardware		$ -	
				Hardware Maintenance		$ -	
				Software License		$ -	
				Solution support		$ 48.94	Represents costs associated with labor activities to support the solution.
Network Access - Static Wired	Schedule 4.3 - Section 5.5	Device	Fixed Monthly Fee Per Unit		$ 55.93		
				Hardware		$ 15.69	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of a combination of 4 and 5 year refresh cycles.
				Hardware Maintenance		$ 11.08	Represents break-fix services, labor and parts.
				Software		$ 1.85	Represents the costs of software licenses upgrades/refresh. Based on a refresh cycle of 4 years on core network systems and 5 years for edge switches, the aggregated cost is apportioned over the baseline volume of Network Access users.
				Software Maintenance		$ 6.46	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 20.86	Represents labor costs for IMAR activities and circuit costs.
Network Access - Static Wired (Library)	Schedule 4.3 - Section 5.5	Device	Fixed Monthly Fee Per Unit		$ 49.77		
				Hardware		$ 15.69	This component represents the costs of acquiring network assets including switches, routers, security & NAC systems and tools. The component fee is comprised of the monthly amortization of a combination of 4 year refresh cycles for routers and security systems and 5 year refresh cycles for switches.
				Hardware Maintenance		$ 11.08	This component represents break-fix services for hardware assets, primarily labor and parts.
				Software		$ 1.85	This component represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems and 5 years for edge switches, the aggregated cost is apportioned over the baseline volume of Network Access users.
				Software Maintenance		$ 6.46	This component represents costs associated with the labor and resources for Level 2 software support.
				IMAR		$ 11.66	This component represents labor costs for IMAR activities
				Circuit		$ 3.03	Residual circuits costs
Uninterrupted Power Supply Support Services	Schedule 4.3 - Section 5.5	Device	Fixed Monthly Fee Per Unit		$ 110.00		
				Hardware			
				Hardware maintenance			

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software		$ 82.50	Represents costs associated with monitoring platform
				Software maintenance		$ 24.20	Represents costs associated with maintenance of monitoring platform and labor to support Break/Fix activities
				IMAR's		$ 3.30	Represents costs associated with IMARs for the addition of new devices for support
Virtual Private Network Access - Level 1	Schedule 4.3 - Section 5.6	Active Account	Fixed Monthly Fee Per Unit		$ 9.40		
				Hardware		$ 2.35	This component represents the costs of acquiring network assets including routers, VPN concentrators, Application Persistence servers, security & NAC systems and tools. The component fee is comprised of the monthly amortization of a combination of 4 year refresh cycles for routers and security systems.
				Hardware Maintenance		$ 1.70	This component represents break-fix services, primarily labor and parts.
				Software		$ 0.36	This component represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems.
				Software Maintenance		$ 1.17	This component represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 0.95	This component represents labor costs for IMAR activities.
				Circuits		$ 2.88	This component represents the cost for intersite bandwidth facilities and Internet access.
Virtual Private Network Access - Level 2	Schedule 4.3 - Section 5.6	Active Account	Fixed Monthly Fee Per Unit		$ 10.91		
				Hardware		$ 1.78	Represents the cost of incremental hardware not included in Infrastructure Services.
				Hardware Maintenance		$ 0.86	Represents break-fix services, primarily labor and parts, not included in Infrastructure Services.
				Software		$ 0.32	Represents the costs of software license acquisition and management.
				Software Maintenance		$ 5.59	Represents software maintenance costs and labor and resources for Level 2 support.
				IMAR's		$ 2.36	Represents labor costs for IMAR activities.
				Circuits		$ -	N/A
Portal - External Users	Schedule 4.3 - Section 5.6	User	Fixed Monthly Fee Per Unit		$ 8.00		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ 4.00	Represents the cost of software license upgrades/refresh.
				Software Maintenance		$ 1.90	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR		$ 2.10	Represents labor costs for IMAR activities.
Portal - Portfolio Application	Schedule 4.3 - Section 5.6	Application	Fixed Monthly Fee Per Unit		$ 210.90		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ 110.00	Represents the cost of software license upgrades/refresh.
				Software Maintenance		$ 70.90	Represents costs associated with the labor and resources for Software Maintenance support.
				Break Fix		$ 30.00	Represents labor costs for Break Fix activities.
GSMS Short Code Setup	Schedule 4.3 - Section 5.7	Event	Fixed Fee Per Unit		$ 3,700.00		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 3,700.00	Represents the license cost attributable to providing GSMS Short Code Setup.
				Software maintenance		$ -	N/A
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
GSMS Short Code Support	Schedule 4.3 - Section 5.7	Month	Fixed Monthly Fee Per Unit		$ 1,507.63		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ -	N/A
				Software maintenance		$ 1,507.63	Represents the software maintenance cost (e.g. patches, upgrades) attributable to providing GSMS Short Code Support.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
GSMS Messages	Schedule 4.3 - Section 5.7	Message	Fixed Fee Per Unit		$ 0.028		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 0.028	Represents the license cost attributable to providing GSMS Messages.
				Software maintenance		$ -	N/A
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
IP Conference Phone	Schedule 4.3 - Section 5.7.3	Phone	Fixed Monthly Fee Per Unit		$ 59.72		
				Hardware		$ 27.87	This component represents the costs of Enterprise voice systems comprised of multiple geo-redundant server clusters, IP infrastructure, gateways, IP Conference Phone, and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles.
				Hardware Maintenance		$ 6.60	Represents break-fix services, primarily labor and parts.
				Software		$ 2.20	Represents the costs of software licenses upgrades/refresh based on the refresh cycle of 5 years
				Software Maintenance		$ 2.20	Represents software programming support
				IMAR's		$ 12.95	represents the labor costs for IMAR activities
				Circuits		$ 7.90	Represents the cost for bandwidth and circuitry
Virtual Phone - Microsoft (MS) Teams Phone	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee per Unit		$ 16.85		
				Hardware		$ 2.56	This component represents the costs associated with the hardware required to deploy and operated the AT&T provided Direct Routing solution
				Hardware maintenance		$ 0.26	This component represents break-fix services for enterprise direct routing hardware
				Software		$ 8.36	This component represents cost system and application software, include Microsoft Teams phone license, required to provide direct routing
				Software maintenance		$ 0.19	This component represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 5.48	This component represents labor and support costs for the Direct Routing solution
				Circuits		$ -	
Voice-Avaya Legacy Support	Schedule 4.3 - Section 5.7.3	Month	Fixed Monthly Fee Per Unit		$ 416,688.00		
				Hardware		$ 114,006.35	This component represents enterprise costs of voice system hardware which are fixed
				Hardware maintenance		$ 34,842.50	This component represents break-fix services for enterprise voice hardware
				Software		$ 92,977.50	This component represents the costs of Enterprise voice systems comprised of multiple geo-redundant server clusters, gateways and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles.
				Software maintenance		$ 27,242.02	This component represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 105,105.30	This component represents labor and support costs for Voice Services which are fixed
				Circuits		$ 42,514.33	This component represents the proportion of Voice Services costs of enterprise circuits
Voice Analog Line	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee Per Unit		$ 47.55		
				Hardware		$ 14.99	Represents the costs of Enterprise voice systems comprised of multiple geo-redundant server clusters, analog to IP adapters, gateways and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles.
				Hardware Maintenance		$ 4.44	Represents break-fix services, primarily labor and parts.
				Software		$ 2.22	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of telephones.
				Software Maintenance		$ 2.22	Represents costs associated with the labor and resources for Level 2 support.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				IMAR's		$ 18.78	Represents labor costs for IMAR activities.
				Circuits		$ 4.90	Represents the cost for intersite bandwidth facilities and PSTN access.
Voice Single-Line	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee Per Unit		$ 22.84		
				Hardware		$ 6.46	This component represents enterprise costs of voice system hardware which are user volume sensitive. It is comprised of telephone sets and cabling hardware
				Hardware maintenance		$ 0.78	This component represents break-fix services, primarily labor and parts
				Software			
				Software maintenance			
				IMAR's		$ 10.35	This component represents labor and support costs for Voice Services which are volume sensitive
				Circuits		$ 5.25	This component represents the proportion of Voice Services costs of enterprise circuits for intersite bandwidth facilities and PSTN access
Voice Multi-Line	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee Per Unit		$ 25.05		
				Hardware		$ 6.33	This component represents enterprise costs of voice system hardware which are user volume sensitive. It is comprised of telephone sets and cabling hardware
				Hardware maintenance		$ 0.77	This component represents break-fix services, primarily labor and parts
				Software			
				Software maintenance			
				IMAR's		$ 10.18	This component represents labor and support costs for Voice Services which are volume sensitive
				Circuits		$ 7.77	This component represents the proportion of Voice Services costs of enterprise circuits for intersite bandwidth facilities and PSTN access
Cloud Access Security Broker	Schedule 4.3 - Section 5.8	Month	Fixed Monthly Fee Per Unit		$ 15,450.12		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 14,350.12	Represents the license cost attributable to providing CASB capability
				Software maintenance		$ 1,100.00	Represents the cost associated with the support of the CASB capability
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
Town Hall Services	Schedule 4.3 - Section 5.9	Event	Fixed Fee Per Unit		$ 76,730.20		
				Hardware		$ 13,920.45	12+ VM Servers with Storage Area Network and 4 Video Network Edge appliances (CDN). 5 Year Refresh cycle included.
				Hardware Maintenance		$ 1,962.50	Cloud based and premise based, the 12+ Servers are Cloud based and the VNEs are premise based.
				Software		$ 37,204.55	AVMS/QUMU application license and VNE/CDN licenses. 5 year refresh cycle included.
				Software Maintenance		$ 4,665.43	Application, Content Distribution and Portal support.
				IMAR's		$ 17,045.45	Townhall administrator and Portal updates.
				Circuits		$ 1,931.82	Origination and distribution bandwidth. Originator connectivity limited to available facilities.
Video Conferencing Services - Personal	Schedule 4.3 - Section 5.9	System	Fixed Monthly Fee Per Unit		$ 315.70		
				Hardware		$ 112.72	Represents the costs of VTC roll-about system codec and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 30.64	Represents break-fix services, primarily labor and parts.
				Software		$ 13.19	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for VTC systems, the aggregated cost is apportioned over the baseline volume of VTC end points.
				Software Maintenance		$ 33.94	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 37.51	Represents labor costs for IMAR activities.
				Circuits		$ 87.69	Represents the cost for intersite bandwidth facilities, Internet and PSTN access.
Video Conferencing Services - Room System	Schedule 4.3 - Section 5.9	System	Fixed Monthly Fee Per Unit		$ 895.13		

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware		$ 300.90	Represents the costs of VTC room system codecs and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 96.25	Represents break-fix services, primarily labor and parts.
				Software		$ 37.40	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for VTC systems, the aggregated cost is apportioned over the baseline volume of VTC end points.
				Software Maintenance		$ 96.25	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 106.35	Represents labor costs for IMAR activities.
				Circuits		$ 257.98	Represents the cost for intersite bandwidth facilities, Internet and PSTN access.
Webex Video Conferencing Services	Schedule 4.3 - Section 5.9	Subscription	Fixed Monthly Fee Per Unit		$ 47.86		
				Software License		$ 43.12	Cost to acquire the Software subscription
				Labor		$ 4.74	IMAR and service administration
Video Streaming and Archiving Services	Schedule 4.3 - Section 5.10	System	Fixed Monthly Fee Per Unit		$ 7,210.62		
				Hardware		$ 1,110.97	Represents the switching and router costs of a dedicated VLAN for Video Streaming services and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles for the switch and 4 year refresh cycles for the router.
				Hardware Maintenance		$ 902.30	Represents break-fix services, primarily labor and parts.
				Software		$ 88.81	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for the switch and 4 years for the router, the aggregated cost is apportioned to a single encoder.
				Software Maintenance		$ 902.30	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 1,540.17	Represents labor costs for IMAR activities.
				Circuits		$ 2,666.06	Represents the cost for intersite bandwidth facilities and Internet access.
Video Streaming - COC Chambers	Schedule 4.3 - Section 5.10	System	Fixed Monthly Fee Per Unit		$ 1,210.00		
				Hardware		$ 186.34	Represents the switching and router costs of a dedicated VLAN for Video Streaming services and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles for the switch and 4 year refresh cycles for the router.
				Hardware Maintenance		$ 151.25	Represents break-fix services, primarily labor and parts.
				Software		$ 18.15	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for the switch and 4 years for the router, the aggregated cost is apportioned to a single encoder.
				Software Maintenance		$ 150.04	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 260.15	Represents labor costs for IMAR activities.
				Circuits		$ 444.07	Represents the cost for intersite bandwidth facilities and Internet access.
Wireless Access Point	Schedule 4.3 - Section 5.12	Device	Fixed Monthly Fee Per Unit		$ 160.18		
				Hardware		$ 51.26	This component represents the costs of acquiring WiFi access assets including a Wireless Access Point and a proportional amount of redundant controllers/NAC and support the Refresh tasks. The component fee is comprised of the monthly amortization of 3 year refresh cycles.
				Hardware Maintenance		$ 30.43	This component represents break-fix services, primarily labor and parts.
				Software		$ 18.69	This component represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 3 years for WiFi network systems, the aggregated cost is apportioned over the baseline volume of Wireless Access Points.
				Software Maintenance		$ 46.45	This component represents costs associated with the labor and resources for Level 2 support and the County WAN/LAN connectivity.
				IMAR's		$ 13.35	This component represents labor costs for IMAR activities.
Network Access - Wire/Wireless	Schedule 4.3 - Section 5.12	Active Account	Fixed Monthly Fee Per Unit		$ 66.68		
				Hardware		$ 16.97	Represents the costs of acquiring network assets including switches, routers, security & NAC systems and tools. The component fee is comprised of the monthly amortization of a combination of 4 year refresh cycles for routers and security systems and 5 year refresh cycles for switches.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware Maintenance		$ 12.59	Represents break-fix services, labor and parts.
				Software		$ 2.91	Represents the costs of software licenses upgrades/refresh. Based on a refresh cycle of 4 years on core network systems and 5 years for edge switches, the aggregated cost is apportioned over the baseline volume of Network Access users.
				Software Maintenance		$ 6.78	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 5.57	Represents labor costs for IMAR activities.
				Circuits		$ 21.86	Represents the cost for intersite bandwidth facilities and Internet access.
3rd-Party Network Access - Category 1	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 536.92		
				Hardware		$ 198.41	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 4 year refresh cycles.
				Hardware Maintenance		$ 103.77	Represents break-fix services, labor and parts.
				Software		$ 30.79	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems, the aggregated cost is apportioned over the baseline volume of 3rd Party Network Access users.
				Software Maintenance		$ 131.04	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 72.91	Represents labor costs for IMAR activities.
3rd-Party Network Access - Category 2	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 544.44		
				Hardware		$ 198.38	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 4 year refresh cycles.
				Hardware Maintenance		$ 103.75	Represents break-fix services, labor and parts.
				Software		$ 30.78	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems, the aggregated cost is apportioned over the baseline volume of 3rd Party Network Access users.
				Software Maintenance		$ 139.77	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 71.76	Represents labor costs for IMAR activities.
3rd-Party Network Access - Category 3	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 548.74		
				Hardware		$ 198.91	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 4 year refresh cycles.
				Hardware Maintenance		$ 104.03	Represents break-fix services, primarily labor and parts.
				Software		$ 30.87	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems, the aggregated cost is apportioned over the baseline volume of 3rd Party Network Access users.
				Software Maintenance		$ 138.36	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 76.58	Represents labor costs for IMAR activities.
3rd Party Network Access - IP Sec - 5 Mbps	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 255.85		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 243.59	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.26	Represents labor costs for IMAR activities.
3rd Party Network Access - IP Sec - 10 Mbps	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 427.31		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 414.97	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.33	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (1 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 153.51		

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 141.25	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.26	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (2 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 260.12		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 247.85	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.26	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (3 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 373.93		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 361.84	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.09	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (4 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 473.32		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 458.80	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 14.53	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (5 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 613.55		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 599.04	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 14.52	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (6-10 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 1,155.51		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 1,127.07	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 28.45	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (20 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 1,907.15		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 1,850.34	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.81	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (30 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 2,504.79		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software		$ -	N/A
				Software Maintenance		$ 2,447.97	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.82	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (40 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 2,879.77		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 2,822.95	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.82	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (50 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 3,032.09		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 2,975.27	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.82	Represents labor costs for IMAR activities.
3rd Party Network Access – Microsoft Teams Rooms	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 359.17		
				Hardware			
				Hardware Maintenance			
				Software			
				Software Maintenance		$ 334.35	This component represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR		$ 24.82	This component represents labor costs for IMAR activities.
				Circuit			
External DNS Management	Schedule 4.3 - Section 5.14	Month	Fixed Monthly Fee Per Unit		$ 28,373.54		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ 1,340.21	N/A
				Software Maintenance		$ 25,804.16	Represents costs associated with the labor and resources for Level 2 support and access bandwidth. Also includes the cost of Akamai service.
						$ 1,229.17	Represents labor costs for IMAR activities.
External DNS Management Enhancement	Schedule 4.3 - Section 5.14	Month	Fixed Monthly Fee Per Unit		$ 28,373.54		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Platform Support		$ 1,340.21	Monitor Bot Management dashboard and respond to incidents.
				Software Maintenance		$ 25,804.16	Represents costs associated with the labor and resources for Level 2 support related to the Kona Security and Bot Management services.
				IMAR's		$ 1,229.17	Represents labor costs for IMAR activities.
New Site Install - Type I Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 232,875.88		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 232,875.88	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
New Site Install - Type II Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 116,437.94		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 116,437.94	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type III Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 80,073.31		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 80,073.31	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type IV Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 67,793.32		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 67,793.32	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type V Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 16,791.25		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 16,791.25	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type VI Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 3,197.05		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 3,197.05	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
Interactive Voice Services - Small	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 687.50		
				Hardware		$ 37.18	Represents the costs of acquiring IP PBX systems that provide Auto Attendant and ACD functions with Contact Management Services and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 136.57	Represents break-fix services, primarily labor and parts.
				Software		$ 74.39	Represents the costs of software licenses upgrades/refresh and programming. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of IVS systems.
				Software Maintenance		$ 222.72	Represents costs associated with the labor and resources for Level 2 support.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				IMAR's		$ 88.43	Represents labor costs for IMAR activities.
				Circuits		$ 128.20	Represents the cost for intersite bandwidth facilities and PSTN access.
Interactive Voice Services - Medium	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 2,722.50		
				Hardware		$ 147.22	Represents the costs of acquiring IP PBX systems that provide Auto Attendant and ACD functions with Contact Management Services with Virtual Wall Boards, Automated Call Recording infrastructure and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 540.83	Represents break-fix services, primarily labor and parts.
				Software		$ 294.60	Represents the costs of software licenses such as Automatic Call Recording, Virtual Wall Boards and Agent Softphones, upgrades/refresh and programming. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of IVS systems.
				Software Maintenance		$ 881.99	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 350.17	Represents labor costs for IMAR activities.
				Circuits		$ 507.68	Represents the cost for intersite bandwidth facilities and PSTN access.
Interactive Voice Services - Large	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 8,234.60		
				Hardware		$ 445.31	Represents the costs of acquiring IP PBX systems that provide Auto Attendant and ACD functions with Contact Management Services with Wall Boards, Integrated Voice Response (IVR), Computer-Telephony Interface (CTI), Short Message Service (SMS), Work Force Management (WFM) and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 1,635.82	Represents break-fix services, primarily labor and parts.
				Software		$ 891.06	Represents the costs of software licenses including IVR, CTI, SMS and WFM, upgrades/refresh and programming. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of IVS systems.
				Software Maintenance		$ 2,667.71	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 1,059.15	Represents labor costs for IMAR activities.
				Circuits		$ 1,535.56	Represents the cost for intersite bandwidth facilities and PSTN access.
Interactive Voice Services - Support for County Retained	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 616.58		
				Hardware		$ 42.87	Represents the costs of acquiring PBX trunking hardware and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 59.45	Represents break-fix services, labor and parts.
				Software		$ 1.14	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of County owned IVS systems.
				Software Maintenance		$ 30.87	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 53.27	Represents labor costs for IMAR activities.
				Circuits		$ 428.98	Represents the cost for intersite bandwidth facilities and PSTN access.
FirstNet Mobility Services	Schedule 4.3 - Section 5.18	Device	Fixed Monthly Fee Per Unit		$ 31.49		
				Support Services		$ 2.06	Includes billing and admin support
				NASPO based carrier plan		$ 29.43	Represents the carrier costs with Taxes and Surcharges included
FirstNet Mobility Services - Tethered	Schedule 4.3 - Section 5.18	Device	Fixed Monthly Fee Per Unit		$ 36.60		
				Support Services		$ 2.06	Includes billing and admin support
				NASPO based carrier plan		$ 34.54	Represents the carrier costs with Taxes and Surcharges included
Mobility Services Hot Spot	Schedule 4.3 - Section 5.18	Device	Fixed monthly fee per unit		$ 25.58		
				Support Services		$ 2.06	Includes billing and admin support
				NASPO based carrier plan		$ 23.52	Represents the carrier costs with Taxes and Surcharges included

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
Citrix Account	Schedule 4.3 - Section 6	Account	Fixed Monthly Fee Per Unit		$ 20.68		
				Hardware		$ 8.05	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware Maintenance		$ 7.39	Represents break-fix services, primarily labor and parts, including reporting activities.
				Software Licenses		$ 1.55	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years.
				Software Maintenance		$ 3.69	Represents costs associated with the labor and resources for Software Maintenance support.
Virtual Guest Server - Cloud IaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Per Unit		$ 551.27		
				Hardware		$ -	N/A
				Operating System License		$ 38.59	Represents the cost of software license upgrades/refresh.
				Other Software License		$ 27.56	Represents an allocation of corporate tools charges.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 485.12	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Cloud PaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Per Unit		$ 413.45		
				Hardware		$ -	N/A
				Operating System License		$ -	N/A
				Other Software License		$ 20.67	Represents an allocation of corporate tools charges.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 392.78	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Clonetab Solution	Schedule 4.3 - Section 6	Month	Fixed Monthly Per Unit		$ 6,211.24		
				Hardware		$ 263.32	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 18.81	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Storage		$ 5,270.83	Represents the storage costs necessary to implement the solution
				Other Software License		$ 28.21	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 39.50	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 590.58	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
DIMSNET Solution	Schedule 4.3 - Section 6	Month	Fixed Monthly Fee Per Unit		$ 15,369.32		
				Hardware		$ 1,873.96	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 113.76	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Storage		$ 9,681.66	Represents the storage costs necessary to implement the solution
				Other Software License		$ 170.62	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 281.10	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 3,248.22	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
WildFire Scanning Service	Schedule 4.3 - Section 6	Month	Fixed Monthly Fee Per Unit		$ 6,658.80		
				Hardware		$ 510.81	Represents the hardware costs, installation and monthly cost for the duration of the service.
				Hardware Maintenance		$ -	
				Software License		$ 5,223.43	Represents the costs related to the third party software subscription services
				Platform support		$ 924.56	Represents costs associated with monitoring activities and responding to incidents.
NetBackup Solution	Schedule 4.3 - Section 6	Month	Fixed Monthly Fee Per Unit		$ 107,963.65		
				Hardware		$ 86,631.99	Represents the hardware, hardware maintenance and software subscription cost.
				Hardware Maintenance		$ -	

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software License		$ -	Represents the costs related to the third party software subscription services
				Solution support		$ 21,331.66	Represents costs associated with labor activities to support the solution.
Mainframe	Schedule 4.3 - Section 6.6	CPU Hour***	Fixed Monthly Fee Per Unit		$ 96.63		
				Hardware		$ -	N/A
				Operating System License		$ 20.29	Represents the cost of software license upgrades/refresh. The aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 3.87	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 72.47	Represents costs associated with operating system license maintenance and the labor and resources for Level 2 support.
AS/400	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 3,118.66		
				Hardware		$ -	N/A
				Operating System License		$ -	N/A
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 1,746.45	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 1,372.21	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Copia Fax Line	Schedule 4.3 - Section 6.7	Fax Line	Fixed Monthly Fee Per Unit		$ 125.00		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ -	N/A
				Software Maintenance		$ -	N/A
				Circuits		$ 125.00	Represents the cost for intersite bandwidth facilities and PSTN access.
Low Code Application Platform - OutSystems	Schedule 4.3 Section 6.7	User	Fixed Monthly Per Unit		$ 54.06		
				Hardware		$ 8.91	Represents the costs associated to the platform cloud hosting.
				Software License		$ 21.17	Represents the software licenses costs of the platform and users licenses.
				Software Maintenance		$ 11.16	Represents vendor support costs.
				Support Labor		$ 12.82	Represents costs associated with platform support.
Oracle Exadata Services - Eighth Rack	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 10,380.95		
				Hardware		$ 4,159.43	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. Exadata X6-2 Eighth Rack 2 x Exadata Server Nodes (22 cores, 512 GB memory each) 18 x Exadata Storage Nodes (43 TB useable - high redundancy) Bare Metal Install
				Hardware (Refresh Labor)		$ 499.19	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 706.67	Represents the labor costs to support the Oracle Exadata servers ,
				Software License		$ 1,200.00	Represents the software license costs to support the Oracle Exadata servers ,
				Hardware Maintenance		$ 2,495.66	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 1,320.00	Represents costs associated with various software maintenance costs.
Oracle Exadata Services - Backup and Recovery	Schedule 4.3 - Section 6.7	Used Terabyte	Fixed Monthly Fee Per Unit		$ 122.88		
				Hardware		$ 32.81	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Operating System License		$ 2.97	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 9.93	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ 10.81	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 66.36	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Oracle Exadata X8M - Production	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 40,951.09		
				Hardware		$ 8,811.20	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. - Exadata X8M -2 Quarter Rack - 2 x Exadata Server Nodes (48 cores, 1.5 TB memory each) - Each of the 3 High Capacity Storage Cells includes: - 36 x 14 TB disk drives, 1.5 TB of Persistent Memory - 504 TB of raw disk space - 150 TB of usable with High Redundancy ASM storage
				Hardware (Install/Refresh Labor)		$ 274.32	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 1,452.05	Represents the labor costs to support the Oracle Exadata servers.
				Software license		$ 10,962.28	Represents the software license costs to support the Oracle Exadata servers, including Oracle Active Data Guard and Advanced Security.
				Hardware Maintenance & Hosting		$ 7,262.54	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 12,188.70	Represents costs associated with various software maintenance costs, including Oracle Active Data Guard and Advanced Security.
Oracle Exadata X8M - Development / Test	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 33,503.21		
				Hardware		$ 8,811.20	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. - Exadata X8M -2 Quarter Rack - 2 x Exadata Server Nodes (48 cores, 1.5 TB memory each) - Each of the 3 High Capacity Storage Cells includes: - 36 x 14 TB disk drives, 1.5 TB of Persistent Memory - 504 TB of raw disk space - 150 TB of usable with High Redundancy ASM storage
				Hardware (Install/Refresh Labor)		$ 274.32	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 1,452.05	Represents the labor costs to support the Oracle Exadata servers.
				Software license		$ 7,435.62	Represents the software license costs to support the Oracle Exadata servers, including Advanced Security.
				Hardware Maintenance & Hosting		$ 7,262.54	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 8,267.48	Represents costs associated with various software maintenance costs, including Advanced Security.
Oracle Exadata X8M - Business Continuity	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 41,268.64		
				Hardware		$ 9,082.07	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. - Exadata X6-2 Quarter Rack - 2 x Exadata Server Nodes (48 cores, 1.5 TB memory each) - Each of the 3 High Capacity Storage Cells includes: - 36 x 14 TB disk drives, 1.5 TB of Persistent Memory - 504 TB of raw disk space - 150 TB of usable with High Redundancy ASM storage - Oracle Platinum Gateway Server

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Hardware (Refresh Labor)		$ 292.56	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 1,452.05	Represents the labor costs to support the Oracle Exadata environment.
				Software License		$ 10,962.28	Represents the software license costs to support the Oracle Exadata servers, including Oracle Active Data Guard and Advanced Security.
				Hardware Maintenance		$ 7,290.97	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 12,188.70	Represents costs associated with various software maintenance costs, including Oracle Active Data Guard and Advanced Security.
Physical Server UNIX - Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 4,878.56		
				Hardware		$ 2,000.22	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 73.18	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 48.79	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 487.85	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 2,268.53	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server UNIX - Medium	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 2,894.99		
				Hardware		$ 1,331.70	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 57.90	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 43.42	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 202.65	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 1,259.31	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server UNIX - Small	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,811.71		
				Hardware		$ 724.69	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 36.23	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 36.23	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 289.88	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 724.68	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server UNIX - X-Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 5,238.56		
				Hardware		$ 2,147.81	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 78.58	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 52.39	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 523.85	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 2,435.93	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Unix - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 4,976.63		
				Hardware		$ 2,040.42	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 74.65	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 49.77	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 497.66	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software Maintenance		$ 2,314.13	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,676.75		
				Hardware		$ 586.86	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 33.53	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 50.30	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 88.03	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 918.02	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - Medium	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,167.08		
				Hardware		$ 350.12	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 23.34	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 35.01	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 52.52	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 706.08	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - Small	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 940.41		
				Hardware		$ 263.32	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 18.81	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 28.21	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 39.50	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 590.58	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - X-Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,960.86		
				Hardware		$ 856.80	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 33.53	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 50.30	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 102.20	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 918.02	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,862.82		
				Hardware		$ 813.96	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 31.86	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 47.79	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 97.09	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 872.12	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Windows	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 616.08		
				Hardware		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Operating System License		$ 43.13	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 30.80	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 542.15	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Windows - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 585.28		
				Hardware		$ -	N/A
				Operating System License		$ 40.97	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 29.26	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 515.05	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Unix	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,293.77		
				Hardware		$ -	N/A
				Operating System License		$ 90.56	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 38.81	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 1,164.39	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Unix - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,229.08		
				Hardware		$ -	N/A
				Operating System License		$ 86.04	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 36.87	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 1,106.17	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Linux	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 646.88		
				Hardware		$ -	N/A
				Operating System License		$ 45.28	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 32.34	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 569.26	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 614.54		
				Hardware		$ -	N/A
				Operating System License		$ 43.02	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 30.73	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software Maintenance		$ 540.79	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Host Server - Windows/Linux	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 5,328.61		
				Hardware		$ 2,930.74	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 106.57	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 159.86	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 498.00	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 1,633.44	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Host Server - Windows / Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 5,062.18		
				Hardware		$ 2,784.20	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 101.24	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 151.87	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 473.10	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 1,551.77	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Acclaim Riverbed	Schedule 4.3 - Section 6.8	Server	Fixed Monthly Fee Per Unit		$ 1,905.36		
				Hardware		$ 854.43	Represents the hardware costs, architecture, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ -	n/a
				Operating System License		$ -	n/a
				Other Software License		$ -	n/a
				Hardware Maintenance		$ 720.93	Represents the third party costs to maintain the hardware.
				Support Labor		$ 330.00	Represents Contractor labor to install and break fix the hardware.
						$ -	n/a
Infrastructure Services	Schedule 4.3 – Section 6.8	Month	Fixed Monthly Fee Per Unit		$ 325,304.45		
				Service Desk Services		$ -	N/A
				End User Services		$ 84,836.57	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Infrastructure Services in support of End User Services.
				Network Services		$ 165,829.28	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Infrastructure Services in support of Network Services.
				Data Center Services		$ 74,638.60	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Infrastructure Services in support of Data Center Services.
				Application Maintenance & Operations Services		$ -	N/A
				Application Development Services		$ -	N/A
				Hardware		$ 151,635.62	Represents the hardware cost of the Routers, Switches and circuit costs, Servers. Refresh has been included based on depreciation period shown on Exhibit 16.1-1.
				Software		$ 45,891.24	Represents the software costs associated with Infrastructure hardware and Software to run the environment.
						$ 127,777.59	Represents the Labor to support Infrastructure Services as defined in Section 2.8 of the Technical Proposal.
Development & Test Services	Schedule 4.3 - Section 6.9	Month	Fixed Monthly Fee Per Unit		$ 223,622.34		
				Service Desk Services		$ -	N/A
				End User Services		$ -	N/A
				Network Services		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Data Center Services		$ -	N/A
				Application Maintenance & Operations Services		$ 79,074.75	Represents the portion of Dev and Test services attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 144,547.59	Represents the portion of Dev and Test services attributable to providing Application Development Services.
				Hardware		$ 88,183.39	Represents the hardware cost of the Routers, Switches and circuit costs, Servers to support the Development and Test environment. Refresh has been included based on depreciation period shown on Exhibit 16.1-1.
				Software		$ 25,007.28	Represents the software costs associated with Development and Test Services Software.
				Labor		$ 110,431.67	Represents the Labor to support Development and Test Environment as defined in Section 2.8 of the Technical Proposal.
Virtual Fax	Schedule 4.3 - Section 6.10	Account	Fixed Monthly Fee Per Unit		$ 38.28		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ -	Represents the cost of software license upgrades/refresh.
				Other Software License		$ 27.05	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 7.03	Represents costs associated with software maintenance along with the labor and resources for support by vendor and Contractor.
				IMAR		$ 4.20	Represents the labor costs for IMAR activities.
Attached Storage – AS/400	Schedule 4.3 – Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.695		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System license		$ -	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	Represents the estimate of the Non-OS License Software
				Hardware maintenance		$ 0.185	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software maintenance		$ 0.510	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Attached Storage – Mainframe	Schedule 4.3 – Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 6.73		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System license		$ -	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	Represents the estimate of the Non-OS License Software
				Hardware maintenance		$ 2.09	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software maintenance		$ 4.64	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Attached Storage - Unix	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 1.07		
				Hardware		$ 0.34	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ -	N/A
				Other Software License		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 0.73	Represents costs associated with storage management software, and the labor and resources for Level 2 support.
Attached Storage - WINTEL	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.82		
				Hardware		$ 0.29	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Operating System License		$ -	N/A
				Other Software License		$ -	N/A
				Hardware Maintenance		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Software Maintenance		$ 0.53	Represents costs associated with storage management software, and the labor and resources for Level 2 support.
Storage - Archive Tier	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.30		
				Hardware		$ 0.16	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 0.01	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 0.03	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 0.07	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 0.03	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Primary Tier	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.74		
				Hardware		$ 0.18	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 0.02	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 0.06	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 0.07	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 0.41	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Secondary Tier	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.52		
				Hardware		$ 0.13	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 0.02	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 0.05	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 0.05	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 0.27	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Document Processing Center 1	Schedule 4.3 - Section 6.12	Unit	Fixed Monthly Fee Per Unit		$ 16,579.20		
				Hardware		$ 8,602.76	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years
				Operating System License		$ 1,650.55	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 928.44	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 3,444.79	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 1,952.66	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Document Processing Center 2	Schedule 4.3 - Section 6.12	Unit	Fixed Monthly Fee Per Unit		$ 9,828.00		
				Hardware		$ 5,099.64	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years
				Operating System License		$ 978.43	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 550.37	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 2,042.04	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 1,157.52	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Immutable Tier (1 TB)	Schedule 4.3 - Section 6.12	1 Terabyte	Fixed Monthly Fee Per Unit		$ 638.62		
				Hardware		$ 318.67	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
				Operating System License		$ 180.73	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 49.17	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 90.05	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Immutable Tier (500GB)	Schedule 4.3 - Section 6.12	512 Gigabyte	Fixed Monthly Fee Per Unit		$ 319.31		
				Hardware		$ 159.02	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 90.05	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 24.59	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 45.66	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Enterprise Application Access	Schedule 4.3 - Section 6.26	Month	Fixed Monthly Fee Per Unit		$ 75,117.37		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ -	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 54,000.00	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 21,117.37	Represents costs associated with software maintenance along with the labor and resources for support by vendor and Contractor.
Optional Item Catalog (OIC) - Software Addition	Exhibit 16.1 - Section 10.2	Add	Fixed Fee Per Unit		$ 2,450.00		
				Hardware		$ 221.32	Represents the lab workstations used to test MSI packing.
				Operating System License		$ -	
				Other Software License		$ 48.28	Represents desktop software packaging and installation kit software.
				Hardware Maintenance		$ -	
				Software Maintenance		$ 2,180.40	Represents the labor costs for adding software to the catalog of available software.
Optional Item Catalog (OIC) - Update	Exhibit 16.1 - Section 10.2	Update	Fixed Fee Per Unit		$ 1,400.00		
				Hardware		$ 112.56	Represents the lab workstations used to test MSI packing.
				Operating System License			
				Other Software License		$ 26.15	Represents desktop software packaging and installation kit software.
				Hardware Maintenance			
				Software Maintenance		$ 1,261.29	Represents the labor costs for updating software to the catalog of available software.
Transition Services - Service Desk Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ -		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ -	N/A
Transition Services - Application Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ -		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ -	N/A

Exhibit 16.1-2 Resource Unit Price Decomposition - **Pricing Decomposition valid through December 31, 2023.**

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee	Component Fee	Component Description
Transition Services - End User Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ -		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ -	N/A
Transition Services - Network Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ -		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ -	N/A
Transition Services - Data Center Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ -		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ -	N/A
Transition Services - Cross Functional Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ -		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ -	N/A
Transition Services - Transition Completion	Schedule 2.1	Milestone	Fixed Fee Per Unit		$ 7,212,700.17		
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 7,212,700.17	See TS7 - Completion tab for details.

*Schedule 4.3 Reference includes the Section reference for the specific requirements for this particular Resource Unit but it still includes all general requirements applicable to such Resource Unit in the higher levels of the obligations hierarchy as described in Schedule 4.3. For example, the Resource Unit for Desktop - Standard Workstation includes not only the responsibilities as stated in Section 4.5 of the End-User Services Section of Schedule 4.3, but also the responsibilities in Sections 4.1 through 4.3 of the End-User Services Section, as well as the responsibilities and requirements in Section 1 of Schedule 4.3.
**The mainframe RU unit volumes are based on the R24 CPUs
***With the exception of 2.3.1.4 and 2.3.1.5 and their respective requirements

Exhibit 16.1-3 – Maximum Annual Fee

1. OVERVIEW

Maximum Annual Fee is based on the quantities provided in Exhibit 16.1-1. Contract Year 1 includes the Transition Costs in addition to twelve months of operations.

Contract Year	Maximum Annual Fee
1	**$57,377,735.09**
2	**$172,000,000.00**
3	**$191,000,000.00**
4	**$207,845,282.00**
5	**$207,547,801.00**
6	**$205,822,123.00**
7	**$219,955,694.00**
8	**$222,628,614.00**

END OF EXHIBIT

Exhibit 16.1-4 – Labor Categories

Table of Contents

1. Overview 4

2. APPLICATION SERVICES LABOR CATEGORIES 4

2.1. Acquisition Manager 4

2.2. Application Architect 5

2.3. Application Developer 6

2.4. Application Developer – Associate 8

2.5. Application Test Lead 9

2.6. Application Test Developer 10

2.7. Business Analyst 11

2.8. Database Administrator 12

2.9. Program Manager 14

2.10. Project Manager 15

2.11. Project Scheduler 16

2.12. Systems Analyst 18

2.13. Senior Application Developer 19

2.14. Web Designer 20

2.15. Desktop Engineer 21

2.16. Gate Review Coordinator 21

2.17. Junior Developer 24

2.18. Data Entry Clerk 24

2.19. Senior Curam Interface Architect 26

2.20. Senior Curam Application Developer 28

2.21. Senior Curam Business Analyst 29

2.22. Intern 31

2.23. Applications Developer - Advanced Technology 32

2.24. Network Architect 32

2.25. Network Engineer 33
2.26. Senior Network Engineer 34
2.27. Technology Transition and Adoption Coordinator (T-TAC) 35
2.28. Information Security Engineer 39
3. KEY PERSONNEL LABOR CATEGORIES 41
3.1. Chief Technical Architect (CTA) 41
3.2. Enterprise Application Architect (EAA) 42
3.3. Innovation Officer (IO) 43
4. NAMED PERSONNEL LABOR CATEGORIES 44
4.1. Applications Developer – ERP Principal 44
4.2. Electronic Health Records (EHR) Program Manager 46

1. OVERVIEW

Exhibit 16.1-4 – Labor Categories provides descriptions of billable and non-billable labor categories for this Agreement. The Contractor shall bill the County using the applicable labor category rate as per the role or task(s) performed by personnel. For example, if the task or role being provided by personnel falls within Business Analyst labor category, hours associated with such role or task(s) shall be billed at the Business Analyst labor category rate. Non-billable labor categories describe the qualifications for designated Key Personnel.

Personnel billing to a labor category rate must meet the requirements of said labor category unless otherwise approved by the County.

2. APPLICATION SERVICES LABOR CATEGORIES

2.1. Acquisition Manager

The Acquisition Manager is responsible for the procurement activities necessary for Contract Management to execute procurement. The Acquisition Manager role performs pre-procurement activities (e.g. stack and rank, request for information, market studies) and goes up to coordinating negotiations and ends at the handoff for the actual procurement activates. This includes activities such as research, requirements development, vendor ranking, and assessment. The Acquisition Manager works with various Frameworks and Framework Components such as Contract Management Services, Asset Management, Applications Maintenance and Operations, and Applications Development.

Knowledge, Skills and Abilities:

Knowledge of:

- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Manage Request for Information (RFI) activities
- Manage Request for Proposal (RFP) activities
- Perform market scan for potential solutions or vendors
- Perform portability assessment and recommendations for Cloud Service procurements
- Perform stack & rank of Provider(s) for potential products and/or services
- Establish and maintain cooperative working relationships

- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree and a minimum seven (5) years of experience working on acquisitions and procurement; OR
2. Associate degree with two (2) additional years of experience; OR
3. High school diploma with four (4) additional years of experience.

2.2. Application Architect

An Application Architect serves as the team lead across all architecture domains including Technical, Security, Data and Application. An Application Architect is responsible for defining IT strategy, evaluating technologies, defining standards, designing solution and reference architectures that solve stated business objectives, supporting the development of architectural frameworks and integrating them with coherent and consistent architectural views.

Knowledge, Skills and Abilities:

Knowledge of:

- Business process design techniques
- Platform architectures and network architectures
- Application design, architecture and development
- Entity modeling
- Test planning
- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Lead the overall design of cross-functional, multi-platform, and Web-based application systems; oversees all application system processes
- Lead the application architecture definition / development
- System design and development

- Direct mapping activities on specific technology platforms
- Provide technical guidance to application development teams and consults on integration and conversion activities
- Conduct reviews, and analyzes organizational needs and goals to develop and implement applications
- Assess performance, tuning and capacity requirements to determine key technology decision
- Oversee the activities of the Database Administrator and the Software Configuration Analyst
- High-level entity modeling activities
- Ensure effective software configuration management across applications
- Assesses and effectively manages risks associated with their business objectives
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Conceptual Architecture Diagram, Interface Design Document, System Architecture Study, Vendor Requirements Questionnaire, and Engineering Documents

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and a minimum seven (7) years of experience working on software application development projects, of which (3) years must have been associated with application requirements management; OR
2. Associate degree with two (2) additional years of experience in software application development; OR
3. High school diploma with four (4) additional years of experience in software application development.

2.3. Application Developer

An Application Developer acts under general supervision, and can act in a lead capacity on application assignments, and/or on complex data processing problems.

Knowledge, Skills and Abilities:

Knowledge of:

- Computer programming
- Principles of designing methods of processing data
- Electronic data processing equipment and its capabilities
- Software Development Life Cycle (SDLC) methodology
- Business Process Management (BPM)
- Service Oriented Architecture (SOA)
- Technical report writing
- Statistical methods
- Software engineering disciplines including: Microsoft .NET, J2EE, SharePoint, Business Intelligence
- Current technology and trends in the profession

Skills and Abilities:

- Analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions
- Write complex programs and develop detailed program specifications
- Use programming and scripting languages, vendor packages and software development tool
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Unit Test Plan, Computer Programs, Software Configuration Item List, and Root Cause Analysis Form

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and a minimum three and half (3.5) years of experience working on software application development projects of which two (2) years must be in a single language unless technology precludes it; OR

2. Associate degree with two (2) additional years of experience in software application development; OR
3. High school diploma with four (4) additional years of experience in software application development.

2.4. Application Developer – Associate

An Application Developer – Associate acts under general supervision on projects, enhancements and operational support for various business applications.

Knowledge, Skills and Abilities:

Knowledge of:

- Software Development Life Cycle (SDLC) methodology
- Business Process Management (BPM)
- Service Oriented Architecture (SOA)
- Software engineering disciplines including: Microsoft .NET, J2EE, SharePoint,
- Business Intelligence

Skills and Abilities:

- Analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions
- Write programs from detailed program specifications
- Apply creative thinking in the support of business applications
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Unit Test Plan, Computer Programs, Software Configuration Item List, and Root Cause Analysis Form

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in Computer Science, Systems Engineering or related degrees; OR

2. Associate degree with two (2) years of experience in software application development; OR
3. High school diploma with four (4) years of experience in software application development.

2.5. Application Test Lead

An Application Test Lead provides technical leadership for all testing activities of assigned projects and assigns work to others on the testing team. An Application Test Lead is responsible for the leading the development and implementation of comprehensive test plans to support application development lifecycles.

Knowledge, Skills and Abilities:

Knowledge of:

- Industry standard testing practices
- Current technology and trends in the profession
- Testing processes, testing metrics and testing tool development
- Testing analysis and design and functional and performance models
- Automated testing tools

Skills and Abilities:

- Plan and lead the analysis of the testing requirements of a project in order to define testing strategy
- Define metrics to be collected to monitor the performance and effectiveness of testing
- Identify and recommend improvements to testing methods and standards for a project through an assessment of current testing practices
- Supports implementation of recommended improvements
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: test strategies and plans, complex testing scenarios and test cases, test reports and work assignments

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Master's or equivalent university degree in management information systems or computer science with a minimum of four (4) years of experience delivering multiple testing services to complex projects; OR
2. Bachelor's or equivalent university degree in Computer Science, Systems Engineering or related degrees with additional two (2) years of experience; OR
3. Associate degree with additional four (4) years of experience; OR
4. High school diploma with additional six (6) years of experience.

2.6. Application Test Developer

An Application Test Developer analyzes complex test results from the scripts, reports on test tool and testing progress and results, facilitates defect resolution and documents final test results in order to complete testing engagement. An Application Test Developer is responsible for developing test cases and scripts and other testing tools in order to implement the comprehensive test plans developed by the Application Test Lead and executing test plans to support application development lifecycles, application upgrades and maintenance.

Knowledge, Skills and Abilities:

Knowledge of:

- Industry standard testing practices
- Current technology and trends in the profession
- Testing processes, testing metrics and testing tool development
- Testing analysis and design and functional and performance models
- Automated testing tools

Skills and Abilities:

- Understand requirements, design specifications, and testing strategy to develop test scenarios
- Selects test design techniques and develop testing metrics collection plans in order to plan and prepare for testing
- Develop and validate models and scripts for testing
- Develop and review test summary reports
- Develop technical tools needed to support testing strategy
- Develop technical test plans and technical test scenarios
- Develop and validate technical test specifications and tools
- Evaluate and validate test cases and scripts

- Application testing
- Evaluate test automation tools and validate testing environments in order to develop test specifications and automated testing tools
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: test plans, complex testing scenarios, test scripts, test tools and other automated testing, test cases and test reports

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Master's or equivalent university degree in management information systems or computer science and a minimum of four (4) years of experience delivering multiple testing services to complex projects; OR
2. Bachelor's or equivalent university degree in Computer Science, Systems Engineering or related degrees with additional two (2) years of experience; OR
3. Associate degree with additional four (4) years of experience; OR
4. High school diploma with additional six (6) years of experience.

2.7. Business Analyst

A Business Analyst works closely with County departments to develop and document functional business requirements that serve as the basis for exploration of system-related solutions. The Business Analyst understands, or is able to quickly grasp, the essential functions of a business and is able to produce business requirements documents, use cases, and business justifications; and is capable of developing and analyzing business process reengineering alternatives.

The Business Analyst is able to work with technical staff and solution architects to analyze potential alternatives and add incremental value through development and/or acquisition efforts, including participation in evaluations, selections, test development, organizational change initiatives, etc.

Knowledge, Skills and Abilities:

Knowledge of:

- Principles of Project Management
- County business, and business functions in a specific department, division, or other area of focus
- General understanding of automated solutions and the systems development life-cycle
- Business requirements documentation
- Use Case approach
- Current technology and trends in the profession
- Proficiency in the use of Microsoft Office Products including Visio and Project

Skills and Abilities:

- Strong analytical and problem solving skills
- Perform risk assessment analysis and identify risk mitigation strategies
- Ability to differentiate between as-is business processes/systems and true business objectives (that my encompass other process/system alternatives)
- Ability to contribute to statements of work, collaborating with Systems Analyst or others
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both written and verbal
- Work independently and in a team environment
- Develop following work products: Business Requirements Document, Functional Requirements Document, use cases, and end user guides

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in a technical discipline and a minimum two (2) years of experience working with the specific business function, or a demonstrated capability to work with the business function in a structured process to develop necessary understanding of the business; AND
2. Minimum two (2) years of experience developing business functional requirements and use cases.

2.8. Database Administrator

A Database Administrator is responsible for configuring and maintaining a database(s), and supporting end users. A Database Administrator provides technical knowledge/expertise in the use of the Database Management System(s) including: table structure design, backup/restore/recovery processes and

procedures, performance analysis and tuning, data file sizing, upgrade/patch support, storage allocation, table space allocation, user account management, and may generating SQL scripts.

Knowledge, Skills and Abilities:

Knowledge of:

- Database Performance Tuning
- Database Security
- Database Management
- Data Maintenance
- Operating Systems
- Information Security Policies
- Current technology and trends in the profession

Skills and Abilities:

- Identify database requirements and design proposed systems
- Define database physical structure and functional capabilities, database security, data back-up, and recovery specifications
- Installs revised or new systems
- Maintain database performance by calculating optimum values for database parameters; implementing new releases; completing maintenance requirements; evaluating computer operating systems and hardware products
- Establish and enforce organization standards
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and minimum of six (6) years of experience working as Database Administrator; OR
2. Associate degree with two (2) additional years of experience; OR
3. High school diploma with four (4) additional years of experience.

2.9. Program Manager

A Program Manager directs and manages the most complex programs that consist of multiple projects and work streams. A Program Manager may also be designated for the most complex projects with County approval. Complex projects are defined as having labor costs greater than $2,000,000 (excluding license or hardware costs) or projects so designated by the GITM.

A Program Manager is responsible for managing all activities related to a complex project, including: coordination of resources, inclusive of Contractor internal resources, County resources and third parties/vendors; developing a detailed project plan to monitor and track progress; managing change to project scope, schedule and cost; stakeholder communications; risk management, including assessment of impacts across multiple work streams; performance measurement; organizational change management; and ensuring that the project is on-time, within scope, and within budget.

A Program Manager interacts with all levels of staff within the County as well as its vendors, including senior, upper and executive management.

Knowledge, Skills and Abilities:

Knowledge of:

- Principles of project management
- Management principles and techniques in project planning and administration
- Management techniques to lead project teams
- Methods and practices of budget, schedule preparation and management
- County business and functions
- Current technology and trends in the profession

Skills and Abilities:

- Plan, organize, and direct the activities and tasks of a project
- Coordinate the resources (internal and external) for the execution of projects
- Prepare and present effective oral and written reports to project team, stakeholders, sponsors, steering committee and all levels of management
- Use interdisciplinary teams effectively in the conduct of the project
- Manage project budget and resource allocation

- Reason logically and creatively and use a variety of analytical and research techniques to solve complex problems
- Work within tight deadline
- Establish and maintain cooperative working relationships
- Proficiency in the use of cost and schedule tools
- Proficiency in the use of Microsoft Office Products including Visio and Project

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree and a minimum of 4,500 hours of project management experience within the last five (5) years; OR
2. Associate degree and a minimum of 6,000 hours of project management experience within the last five (5) years; OR
3. High school diploma or equivalent secondary school credential and a minimum of 7,500 hours of project management experience within the last five (5) years; AND
4. Project Management Professional (PMP) certification or equivalent credential with County approval.

2.10. Project Manager

A Project Manager is responsible for the managing all activities related to a project including: coordination of resources, inclusive of Contractor internal resources, County resources and third parties/vendors; developing a detailed project plan to monitor and track progress; managing change to project scope, schedule and cost; stakeholder communications; risk management; performance measurement; and ensuring that project is on-time, within cope and within budget.

A Program Manager interacts with all levels of staff within the County as well as its vendors, including senior, upper and executive management.

Knowledge, Skills and Abilities:

Knowledge of:

- Principles of project management
- Management principles and techniques in project planning and administration

- Management techniques to lead project teams
- Methods and practices of budget, schedule preparation and management
- County business and functions
- Current technology and trends in the profession

Skills and Abilities:

- Plan, organize, and direct the activities and tasks of a project
- Coordinate the resources (internal and external) for the execution of projects
- Prepare and present effective oral and written reports to project team, stakeholders, sponsors, steering committee and all levels of management
- Use interdisciplinary teams effectively in the conduct of the project
- Manage project budget and resource allocation
- Reason logically and creatively and use a variety of analytical and research techniques to solve complex problems
- Work within tight deadline
- Establish and maintain cooperative working relationships
- Proficiency in the use of cost and schedule tools
- Proficiency in the use of Microsoft Office Products including Visio and Project

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree and a minimum of 3,000 hours of project management experience within the last five (5) years; OR
2. Associate degree and a minimum of 4,500 hours of project management experience within the last five (5) years; OR
3. High school diploma or equivalent secondary school credential and a minimum of 6,000 hours of project management experience within the last five (5) years; AND
4. Project Management Plan (PMP) certification or equivalent credential with County approval.

2.11. Project Scheduler

A Project Scheduler develops and maintains project schedules and supports Program Manager with project scheduling and analysis. The Project Scheduler is responsible for implementing standard processes, tools and program planning and control practices for project schedules. The Project Scheduler will communicate

weekly activities that are to occur, and maintain activities according to baseline. The Project Scheduler will also track and report SPI.

Knowledge, Skills and Abilities:

Knowledge of:

- Principles of Project Management
- Critical Path Analysis
- Earned Value Management

Skills and Abilities:

- Develop and maintain Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) detail schedule
- Develop schedules that include project phasing, project milestones, and represent critical relationships between program tasks as required to plan, coordinate, and visualize all significant program activities
- Assess project schedule risks for effective mitigation
- Develop and analyze planning, scheduling and change related metrics/reports, including critical path analysis, resource analysis, etc.
- Analyze trends, develop reports, facilitate communication and provide feedback on performance
- Conduct Earned Value Analysis
- Establish and maintain cooperative working relationships
- Demonstrate good communication skills, both written and verbal; communicate effectively with both technical and non-technical users
- Work independently and in a team environment
- Proficiency in the use of Microsoft Office Products including Visio and Project

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree and a minimum 6 years experience in scheduling and project management; AND
2. Proficiency in Microsoft Project.

2.12. Systems Analyst

A Systems Analyst implements computer system requirements by defining and analyzing system problems; designing and testing standards and solutions. A Systems Analyst is responsible for eliciting, documenting, and analysis of requirements for the development, installation, implementation, procurement, or support of custom developed systems or third party developed systems.

Knowledge, Skills and Abilities:

Knowledge of:

- Principles of Project Management
- Data processing, hardware platforms, and enterprise software applications
- System Design
- Software Development Process, Software Documentation, Software Testing
- County business and functions
- Current technology and trends in the profession
- Proficiency in the use of Microsoft Office Products including Visio and Project

Skills and Abilities:

- Strong analytical and problem solving skills
- Perform risk assessment analysis and identify risk mitigation strategies
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Requirements Document, Project Proposal, Requirements Traceability matrix, and Risk Management Plan

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems and a minimum six (6) years of experience working on software application development projects, of which (3) years must have been associated with application requirements management; OR
2. Associate degree with two (2) additional years of experience in software application development; OR

3. High school diploma with four (4) additional years of experience in software application development.

2.13. Senior Application Developer

A Senior Application Developer creates and updates the most complex applications and/or resolves the most complex data processing problems. A Senior Application Developer is responsible for code design and implementation using system configuration and code to provide solutions.

Knowledge, Skills and Abilities:

Knowledge of:

- Computer programming
- Electronic data processing equipment and its capabilities
- Software development cycle
- Principles of designing methods of processing data
- Technical report writing
- Statistical methods
- Current technology and trends in the profession

Skills and Abilities:

- Analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions
- Write complex programs and develop detailed program specifications
- Use programming and scripting languages, vendor packages and software development tool
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Unit Test Plan, Computer Programs, Software Configuration Item List, and Root Cause Analysis Form

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and a minimum eight (8) years of experience working on software application development projects; OR
2. Associate degree with two (2) additional years of experience in software application development; OR
3. High school diploma with four (4) additional years of experience in software application development.

2.14. Web Designer

A Web Designer designs and builds web sites using a variety of graphics software applications, techniques, and tools. A Web Designer acts under general supervision, and can act in a lead capacity or work independently on application assignments, and/or on complex data processing problems.

Knowledge, Skills and Abilities:

Knowledge of:

- User interface design and development
- Digital imaging
- Web development
- Content management
- Multimedia design
- Multimedia programming and technology (e.g. HTML, Photoshop, Illustrator)
- Current technology and trends in the profession

Skills and Abilities:

- Design webpage layout
- Determine technical requirements
- Update websites
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Unit Test Plan, Computer Programs, Software Configuration Item List, Graphics, and Animation

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and minimum of two (2) years of experience working on software development projects of which at least one (1) year must be in web design; OR
2. Associate degree with two (2) additional years of experience in software development; OR
3. High school diploma with four (4) additional years of experience in software development.

2.15. Desktop Engineer

The Desktop Engineer will support application packaging, deployments, documentation, and release control in an Enterprise environment, and perform baseline image creation for multiple hardware configurations. Provide advice, technical consultation, and guidance to internal teams and external clients by analyzing and resolving problems and evaluating alternative means of satisfying user requirements, research and implement new technology to service the client and the team while staying up to date on the latest solutions, and communicate with the vendors to ensure the best option is provided. Oversee multiple projects and teams to meet project milestones, schedules, and scope in alliance with best practices, identify reoccurring issues, and work with IT and business partners to remediate using the problem management process.

Education and/or Experience:

- 5+ years of experience in a professional work environment
- 18+ months of experience with deploying software in a Windows environment
- BA or BS degree preferred
- Certification in Microsoft Operating Systems or Engineering, including MCSE preferred

2.16. Gate Review Coordinator

The IT PMO Gate Review Coordinator (GRC) role and responsibility is as an active team member in (a) the execution of all project management processes and procedures, and (b) proactive leadership in the review and remediation of all associated artifacts from project inception through final delivery. This role will assure that the mission of each individual project is accomplished as specified by the County of San Diego and ITO.

Knowledge, Skills and Abilities:

- Facilitate Project Gate Review process and procedures as a member of the project team
    - Ensure proper level of tailoring for Gate Review artifacts based upon identified project risk
    - Ensure project team and customer throughout the project life cycle in accordance with the Gate Review schedule
    - Ensure requirements tracking through project life cycle
    - Ensure Project artifact compliance to the Requirements Traceability Matrix (RTM) and track issues and corrective actions
    - Participate in the development of the County Project Evaluation & Classification
    - Tool (CPECT) risk classification tool and assist in the evaluation of results
    - Monitor Project Risk and Opportunities Register
    - Conduct independent risk reviews & monitor/report risk mitigation activities
    - Ensure that 3rd Party Vendor performance and deliverables/artifacts conform to
    - ITO policies and procedures
    - Recommend/Implement lessons learned for continuous improvement

- Review project deliverables and remediate as part of project team
    - Identify potential issues in cost, schedule & technical performance which could
    - Impact project artifacts and deliverables
    - Participate in Work Product Peer Reviews (WPPRs)
    - Review project issue closure plans
- Manage project Gate artifact review and approval workflow
    - Evaluate artifacts prior to Gate Review and coordinate with Project Manager
    - (PM)/Technical Leads on remediation efforts as required
    - Establish/verify the review criteria for each artifact are achieved prior to Gate Review (these criteria are also used during Gate Review)
        - Gate Entry Criteria verification checklist
        - Gate Review Input verification checklist
        - Review criteria and Go/No-Go conditions
    - Ensure Stakeholders have reviewed artifacts and completed templates prior to Gate Review
- Manage project Gate Review process
    - Prepare Schedule/Agenda and notify participants including Gate Review lead-time scheduling for Stakeholders
    - Lead Gate Review and rules of engagement for Gate/Artifacts (Go/No-Go decision)

  - Capture/Verify Gate Review artifact action items with participants during Gate Review and distribute
  - Capture Gate Review attendees, decisions and action items in the designated repository
- Ensure project Gate Review closure
  - Capture final updates on action items and post to designated repository
  - Ensure that Gate Review action items are closed per schedule and report nonconformance to PM

Education and/or Experience:

The GRC will have experience in Mission Assurance developing and applying MA processes and procedures specific to the full project development life cycle. To be considered for this position, the candidate must minimally meet the knowledge, skills, and abilities listed below:

- Bachelor's Degree
- 5 years working in a product engineering and/or a IT service environment with focus on all aspects of the product /service lifecycle to include development, verification, deployment and operation within an IT managed service environment
- 3 years in the analysis of service performance gaps and process improvement
- 3 year experience and demonstrated knowledge of program management processes (e.g., risk management)
- 3 year experience implementing product engineering or IT service (ITIL) processes within a variety of systems or services environments; involving systems or services teams in the definition, documentation, deployment and improvement of processes.
- Candidates with these preferred qualifications will be given preferential consideration:
  - Bachelor's degree in System Engineering or where there is no technical (B.S) degree, post graduate certifications in IT related areas
  - Demonstrated proficiency in communication and/or facilitation skills which will be needed in dealing with a variety of stakeholders across the Operating Unit to include program technical staff, program managers, senior managers and customer representatives
  - Proficiency in all Microsoft Office products

    Certification or extensive experience in system engineering methodologies or frameworks (i.e., CMMI-DEV, ITIL V2 or ITIL V3) which support technical aspects of the program

2.17. Junior Developer

Junior Developers perform technical or business tasks at the direction of an experienced manager or coach. Duties include:

- Assists in the design, coding, and testing of technical solutions.
- Assists in systems requirements analysis, data analysis and engineering, systems design, quality assurance, systems testing, configuration management, and application documentation.
- Prepares reports, manuals and other documentation on the status, operation and maintenance of software.
- Develops simple data queries for existing or proposed databases or repositories.

Knowledge, Skills, and Abilities:

Knowledge of:

- Database software
- Spreadsheets
- Word processing
- Development Methodologies (e.g., Waterfall, Agile, Iterative)
- Proficiency in the development language or environment being used

Skills and Abilities:

- Strong oral and written communication skills

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education I experience:

1. Undergraduate students with major in Computer Science oz related field and GPA of 3.0 or above.
2. Bachelor's Degree in Computer Science or related field.
3. Recent formal technical training with a certificate in application coding, database administration, or other applicable technical training and 2 years or less actual experience.

2.18. Data Entry Clerk

A Data Entry Clerk transfers data from paper formats into computer files or database systems using keyboards, data recorders or optical scanners. Duties include:

- Prepares source data for computer entry by compiling and sorting information; establishing entry priorities.
- Processes source documents by reviewing data; resolves discrepancies by using standard procedures or returning incomplete documents to the team leader for resolution.
- Verifies entered data by reviewing, correcting, deleting, or reentering data; combining data from systems when account information is incomplete; purging files to eliminate duplication of data.
- Complies with data integrity and security policies.
- Maintains client confidence and protects operations by keeping information confidential.
- Retrieves data from the database or electronic files as requested.
- Updates data and deletes unnecessary files.

Knowledge, Skills, and Abilities:

Knowledge of:

- Database software
- Spreadsheets
- Word processing

Skills and Abilities:

- Good typing and numeric key antsy skills.
- Good spelling, grammar, and punctuation skills
- Strong reading comprehension
- Attention to detail

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education /experience:

1. High school diploma
2. Formal computer training
3. Proficient in relevant computer applications such as MS Office
4. Accurate keyboard skills and proven ability to enter data at the required speed
5. Knowledge of clerical and administrative procedures

2.19. Senior Curam Interface Architect

A Senior Curam Interface Architect serves as the team lead across all architecture domains affected by the interface of one system to another. A Senior Curam Interface Architect is responsible for defining IT strategy, evaluating technologies, defining standards, designing solution and reference architectures that solve stated business objectives, in support of system interfaces.

For the ConnectWellSD program, this role will:

- Report to the ES Program Manager
- Interface with the IBM developers to define requirements
- Update technical architecture documents, as needed
- Work with the IBM developers to develop clear specifications
- Signoff on all developer specifications to the ES technical team
- Work with the ES technical team to resolve issues and provide technical direction
- Work with the ES technical team to deliver solutions

Knowledge, Skills and Abilities:

Knowledge of:

- Curam
- IBM's Social Program Management platform
- MDM
- Service Oriented Architecture (SOA), service buses
- Business process design techniques
- Platform architectures and network architectures
- Application design, architecture and development
- Entity modelling
- Test planning
- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Lead the overall design of cross-functional, multi-platform, and Web-based data interfaces
- Lead the interface architecture definition / development
- System design and development
- Direct mapping activities on specific technology platforms

- Provide technical guidance to interface development teams and consults on integration activities
- Conduct reviews, and analyses organizational needs and goals to develop and implement interfaces
- Assess performance, tuning and capacity requirements to determine key technology decision
- Ensure effective software configuration management across applications
- Assesses and effectively manages risks associated with their business objectives
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop following work products: Conceptual Architecture Diagram, Interface Design Document, System Architecture Study, Vendor Requirements Questionnaire, and Engineering Documents

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and a minimum eight (8) years of experience working on software application development projects, of which (3) years must have been associated with application requirements management; OR
2. Associate degree with two (2) additional years of experience in software application development; OR
3. High school diploma with four (4) additional years of experience in software interface development.
4. At least 5 years' experience in system development for an HHSA organization

Restrictions on use:

The use of this Resource Unit is limited to the following:

1. Limited to ConnectWellSD program
2. Limited to maximum of one (1) resources assigned to this RU
3. Requires approval from County for the named resource
4. Cannot be transferred to another ES employee without written County consent

2.20. Senior Curam Application Developer

A Senior Curam Application Developer acts with minimal supervision, and can act in a lead capacity on application assignments, and/or on complex data processing problems.

For the ConnectWellSD program, this role will:

- Report to the ES Program Manager
- Perform Curam team leadership function
- Perform break-fix function, and allocate break-fix work to junior Curam team members
- Perform system enhancements/modifications to requirements
- Identify and implement performance improvements
- Troubleshoot outages and reported system issues
- Mentor and train junior Curam team members

Knowledge, Skills and Abilities:

Knowledge of:

- Computer programming
- Curam
- IBM's Social Program Management platform
- Principles of designing methods of processing data
- Electronic data processing equipment and its capabilities
- Software Development Life Cycle (SDLC) methodology
- Business Process Management (BPM)
- Service Oriented Architecture (SOA)
- Technical report writing
- Statistical methods
- Software engineering disciplines including: Microsoft .NET, J2EE, SharePoint, Business Intelligence
- Current technology and trends in the profession

Skills and Abilities:

- Analyze data and situations, reason logically and creatively, identify problems, draw valid conclusions, and develop effective solutions
- Write complex programs and develop detailed program specifications
- Use programming and scripting languages, vendor packages and software development tool

- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form
- Work independently and in a team environment
- Develop

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and a minimum six (6) years of experience working on software application development projects of which two (2) years must be in a single language unless technology precludes it; OR
2. Associate degree with two (2) additional years of experience in software application development; OR
3. High school diploma with four (4) additional years of experience in software application development.
4. At least 5 years' experience in system development for an HHSA organization

Restrictions on use:

The use of this Resource Unit is limited to the following:

1. Limited to ConnectWellSD program
2. Limited to maximum of two (2) resources assigned to this RU
3. Requires approval from County for the named resource
4. Cannot be transferred to another ES employee without written County consent

2.21. Senior Curam Business Analyst

A Senior Curam Business Analyst works closely with County departments to develop and document functional business requirements that serve as the basis for exploration of system-related solutions. The Senior Curam Business Analyst understands, or is able to quickly grasp, the essential functions of a business and is able to produce business requirements documents, use cases, and business justifications; and is capable of developing and analyzing business process reengineering alternatives.

The Senior Curam Business Analyst is able to work with technical staff and solution architects to analyze potential alternatives and add incremental value through development and/or acquisition efforts, including participation in evaluations, selections, test development, organizational change initiatives, etc.

For the ConnectWellSD program, this role will:

- Report to the ES Program Manager
- Work with the Application Architect to define ConnectWellSD roadmap and strategy
- Advocate the roadmap and strategy to newly engaged HHSA departments
- Guide requirements definition for HHSA departments to meet departmental business needs as well as ConnectWellSD strategic intent
- Identify opportunities in:
    - Overlap of functional requirements between various HHSA departments
    - New functional requirements for future ConnectWellSD scope consideration
- Advise County Program Manager on departmental issues, concerns, and risks
- Propose solutions to identified issues and risks
- Facilitate and improve testing plans to eliminate defects first occurring late in test cycle
- Mentor and train junior ConnectWellSD BAs

Knowledge, Skills and Abilities:

Knowledge of:

- Curam
- IBM's Social Program Management platform
- Principles of Project Management
- County business, and business functions in a specific department, division, or other area of focus
- General understanding of automated solutions and the systems development life-cycle
- Business requirements documentation
- Use Case approach
- Current technology and trends in the profession
- Proficiency in the use of Microsoft Office Products including Visio and Project

Skills and Abilities:

- Strong analytical and problem-solving skills
- Perform risk assessment analysis and identify risk mitigation strategies
- Ability to differentiate between as-is business processes/systems and true business objectives (that may encompass other process/system alternatives)

- Ability to contribute to statements of work, collaborating with Systems Analyst or others
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both written and verbal
- Work independently and in a team environment
- Develop following work products: Business Requirements Document, Functional Requirements Document, use cases, and end user guides

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in a technical discipline and a minimum six (6) years of experience working with the specific business function, or a demonstrated capability to work with the business function in a structured process to develop necessary understanding of the business; AND
2. Minimum two (2) years of experience developing business functional requirements and use cases.
3. At least 5 years' experience in requirements development for an HHSA organization

Restrictions on use:

The use of this Resource Unit is limited to the following:

1. Limited to ConnectWellSD program
2. Limited to maximum of one (1) resource assigned to this RU
3. Requires approval from County for the named resource
4. Cannot be transferred to another ES employee without written County consent

2.22. Intern

An Intern serves to support the Innovation Services program. To be considered for the intern position, a student must be enrolled at a college/university and meet the following requirements:

- Major in Computer Science, Industrial System Engineering, Information Technology, Computer Engineering, or related IT discipline preferred
- Past leadership and/or project management experience
- Community and/or campus involvement
- Interest/experience in information technology; software development expertise is a plus
- Ability to use popular office software and social media
- Ability to perform quantitative and qualitative analytics
- Ability to adapt quickly to a changing environment

- Ability to understand business processes and identify opportunities for improvement
- Ability to learn new concepts and assimilate information

Interns will perform technical or business tasks at the direction of an experienced manager or coach.

Duties include:

- Support Research
- Assist in pilots or proof-of-concepts
- Work and collaborate with technology partners and end-users
- Rapidly learn and leverage technologies

Knowledge, Skills and Abilities:

Knowledge of:

- Web technology applications
- Data Management
- Cloud-based technology

Additional Skills:

- Take direction well and be a motivated self-starter
- Strong oral and written communication skills
- Comfort with team collaboration

2.23. Applications Developer - Advanced Technology

The ADAT labor category is applicable when tasks require a deep understanding of new and emerging technologies and/or in complex application integration projects. Additionally, only pre-approved resources who meet the established qualifications are eligible to charge against the ADAT labor category.

ADAT tasks, qualifications, and pre-approved resources are documented in Schedule 5 Report 165 – ADAT Resource List.

2.24. Network Architect

The Network Architect is responsible for maintaining the design and integrity of the internal network. Provides expert technical assistance to team members on high-level system and networking request. Oversees the coordination, partnerships and management of technology vendors, outside consultants and internal dotted line resources as needed. As subject matter expert in the end to end network, works closely with business partners to identify and quantify business issues associated with specific projects, develop and implement business strategy, and assist in setting strategic technical direction in support of customer facing organizations.

Knowledge, Skills and Abilities:

Knowledge of:

- Current technology and trends in the profession
- County business and functions

Skills and Abilities

- Reviews and approves proposed technical network designs to insure business requirements are met
- Provides leadership for projects, including such activities as developing business cases, defining business and or technical requirements and preparing detailed plans and schedules
- Reviews and interprets technical documentation and vendor specifications for inclusion/ adaptation into network standards
- Proficient in network design

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Qualifying education/experience:

- CNP or higher certification or equivalent experience
- Must have 10+ years of experience focused on Cisco switching and routing technologies
- Expertise in working on large complex enterprise networks

2.25. Network Engineer

The Network Engineer is responsible the implementation and deployment of network hardware and software. Assists in operational testing and implementation of new hardware and configurations.

Knowledge, Skills and Abilities:

Knowledge of:

- Current technology and trends in the profession
- County business and functions
- Hardware and software installation methods and procedures

Skills and Abilities:

- Assists in technical troubleshooting of all network troubles
- Provides field support for break/fix repair of network elements
- Provides installation and support for network projects such as equipment refresh

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Qualifying education/experience:

- CCNA or Higher certification
- Must have 3-5 years of experience focused on Cisco switching and routing technologies
- Expertise in working on different sized networks

2.26. Senior Network Engineer

The Network Engineer is responsible for the overall all day to day monitoring, maintenance, administration, and performance management of specific network elements and services. Assists in the coordination, partnership and management of technology vendors, outside consultants and internal dotted line resources as needed.

Conducts operational laboratory testing and configuration of new hardware and network software. Provides the technical troubleshooting and leadership skills required to recover from the most complex network problems in real time to restore service.

Knowledge, Skills and Abilities:

Knowledge of:

- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Provides the senior level technical troubleshooting of all network troubles
- Implements technical network designs to insure business requirements are met
- Maximizes network performance by monitoring performance; troubleshooting network problems and outages; scheduling upgrades; collaborating with network architects on network optimization
- Assists in development of business cases, defining business and or technical requirements and preparing detailed plans and schedules
- Reviews and interpret technical documentation and vendor specifications for inclusion/ adaptation into network standards

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Qualifying education/experience:

- CCNA or Higher certification
- Must have 5+ years of experience focused on Cisco switching and routing technologies
- Expertise in working on large complex enterprise networks

2.27. Technology Transition and Adoption Coordinator (T-TAC)

The Technology Transition & Adoption Coordinator (T-TAC) will be responsible for outlining, planning, and implementing organizational change to ensure successful transition from current state use of technology to future state use of technology in County of San Diego.

The focus of the T-TAC is to ensure all end-users are prepared for change and realize benefits brought about by system implementations.

The scope will include:

- Establish and support the design, implementation, and evolution of organizational change management strategies and plans to engage, inspire, reduce resistance, increase adoption rates, and motivate people to embrace the significant changes associated with information and technology efforts.
- Conduct impact assessments to evaluate the organizational, cultural, and operational implications of proposed changes associated with information and technology efforts. Collect and evaluate data to synthesize information to report on the progress of all projects to their respective stakeholders and leadership.
- Collaborate with stakeholders at all levels of the organization to identify potential barriers, risks, and challenges associated with technology change initiatives and develop mitigation strategies.
- Advise and provide recommendations to stakeholders on matters of significance by identifying change metrics to track, and coordinate with subject matter experts to build and maintain metrics scorecard for change readiness of projects.
- Conduct impact assessments to evaluate the organizational, cultural, and operational implications of proposed changes associated with information and technology efforts. Collect and evaluate data to synthesize information to report on the progress of all projects to their respective stakeholders and leadership.

- Provide guidance to functional areas, including coordinating with subject matter experts to identify training requirements and designs holistic, integrated training plans to drive adoption of processes and programs while maintaining program standards and ensuring successful transition for end- users.
- Provide coaching and support to leaders and managers to enhance their change leadership capabilities and promote a positive change culture.
- Plan and organize training programs to build change management capabilities within the organization to ensure successful transition for end-users.
- Monitor and measure the effectiveness of change management initiatives, identify areas for improvement, and implement corrective actions as needed.
- Collaborate with cross-functional teams to ensure alignment, consistency, and integration of change activities across the organization.
- Stay up to date with industry best practices, trends, and emerging technologies related to organizational change management associated with information and technology efforts in the context of local government.
- Develop and implement strategic communications plans that promote awareness and understanding of the strategic objectives of IT transformation efforts.
- Build and maintain solid partnerships with project stakeholders to better develop, coordinate, direct, and facilitate strategic communications designed to meet organizational goals.
- Develop content and direct creative execution to provide a consistent, targeted, and impactful messaging to all stakeholders.
- Develop a tailored engagement strategy for each stakeholder group to address their concerns and aid them in becoming champions of change.
- Build and maintain solid partnerships with project stakeholders to better develop, coordinate, direct, and facilitate stakeholder relationships and strategic communications to meet organizational goals.
- Guide and assist with implementing communication plans at project level for information and technology initiatives to ensure goals, values and communication standards are consistently depicted, as needed.

Knowledge, Skills, and Abilities:

The T-TAC will have the following responsibility:

- Program Level Standards and Strategies: Lead the development and support implementation of fit-for-purpose change management strategies to accelerate return on investment; collaborate across

program and technical teams to remain integrated with broader program plans by utilizing proven change management methodologies and techniques.

- Assessments: Guide teams through perform quantitative and qualitative assessments for key stakeholder groups to drive development of data-driven change strategies to facilitate the transformation from "current state" to "desired state" by utilizing proven analytical tools for readiness assessments, impact assessments, risk assessments, performance metrics and balanced scorecards.
- Stakeholder Engagement: Plan, develop, and work with leadership and change networks to deliver communications and creative engagement activities, driving understanding about key changes.
- Communications Development: Work closely with subject matter experts, leadership, and communications offices to develop and drive consistent key program messaging and content including identifying and defining methods and channels to drive organizational changes.
- Training and Capability Building: Work with subject matter experts to organize and facilitate training programs as part of technology transitions and/or adoption for end-users, provide coaching and support to leaders and managers in such matters.
- Change Facilitation: Facilitate meetings, focus groups and listening sessions, develop surveys, and utilize additional methods to conduct stakeholder analyses and identify potential barriers, risks, and challenges associated with change initiatives. Facilitate technology-related organizational change activities across teams, promoting understanding and support for new applications and platforms.
- Industry Best Practices: Stay informed on industry trends / leading best practices around organizational change management as it relates to information and technology efforts in the context of local government and proactively incorporate those leading practices into evolving methodologies, tools, templates, processes, and organizational thinking for continuous improvements.
- Additional Deliverables: Including but not limited to various strategic plans focusing on organizational change, stakeholder engagement, communications, and user adoption.

Qualifications, Education and/or Experience:

The candidate must have the following qualifications:

- Bachelor's degree in organizational leadership or related field.
- Minimum of eight years of experience executing organizational change management initiatives for complex government organizations.
- Prosci® or equivalent change management certification.
- Strong executive presence and the ability to work with and influence senior leaders.

- Experience with information and technology efforts in the context of local government large scale implementations of enterprise-wide platforms or new technology.
- Experience leading major organizational change efforts associated with information and technology in the context of local government or within a public sector organization of similar size and complexity to County of San Diego.
- Proven track record of successfully leading and managing complex organizational change initiatives with measurable outcomes.
- Experience in strategic planning and organizational psychology/development and bringing about successful culture change, including risk assessment and mitigation.
- Experience developing strategic communication plans and demonstrated ability to communicate effectively with a wide variety audience, leveraging modes of communication most appropriate for audience and subject matter, including live presentations, written messages, newsletters, etc.
- Experience in developing training programs and materials in support of change initiatives.
- Demonstrated ability to utilize proven analytical tools for readiness assessments, focus groups, surveys, impact assessments, risk assessments, performance metrics and balanced scorecards.
- Experience leading and facilitating groups, presenting briefings, and working with senior leadership teams.
- Knowledge of competency modeling, job task analysis, training needs assessments, and human capital study methods.
- Strong organizational skills, be detail-oriented and work in an accelerated development environment with ability to plan, prioritize, and make decisions on multiple time-sensitive projects.
- Strategic thinker with ability to make connections across workstreams and matrixed organizations.
- Excellent communication, facilitation, and interpersonal skills, with the ability to effectively collaborate with stakeholders at all levels of the organization.
- Strong project management skills, including the ability to develop and execute organizational change management plans and deliverables on time and within budget.
- Highly skilled in use of Microsoft applications including, but not limited to: Outlook, Word, PowerPoint, Excel, OneDrive, OneNote, Visio, Project, SharePoint, Teams and Publisher.
- Ability to analyze complex problems, identify root causes, and develop creative and practical solutions.
- Knowledge of Health and Human Services operations, processes, and regulations is a plus.

2.28. Information Security Engineer

The Security Engineer is responsible for solution design review, implementation activities, application and infrastructure assessment, compliance enforcement, and identity governance management of internally developed and third-party integrated applications. This includes activities such as vendor assessments, solution assessments, risk assessments, privacy impact assessments, architectural reviews, application/code reviews, infrastructure reviews, compliance reviews and enforcement, role-based identity and access provisioning, research, requirements development, vendor ranking, and assessment. The Information Security Engineer works with various Frameworks and Framework Components such as Contract Management Services, Asset Management, Applications Development, Architecture Development, and Maintenance and Operations. The Information Security Engineer labor category may only be utilized for the performance of services that Contractor is not already required to perform under the Agreement.

Knowledge, Skills and Abilities:

Knowledge of:

- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Participation in vendor review, assessment, contracts, and onboarding activities
- Participation in solution development, review, assessment, and onboarding activities
- Perform security audit (controls tests) activities
- Perform security risk assessments of potential solutions or vendors
- Perform security risk assessments of existing solutions or vendors
- Perform penetration testing activities
- Perform solution or vendor regulatory and standards compliance assessments
- Perform solution vulnerability scanning assessments
- Perform solution threat modeling assessments
- Perform secure coding assessments
- Perform application integration of single sign-on activities
- Perform implementation of role-based access provisioning
- Perform role-based and least privilege access assessments
- Design, build, review, and implement infrastructure and application security audit logging changes
- Perform CIS benchmark hardening activities

- Perform Enterprise environment baseline hardening activities (implementation of guardrails, security controls, policies) (e.g. AWS cloud)
- Design, build, review and implement Active Directory Schema, User Object, Device Object, and Group Policy changes
- Design, build, review, and implement enterprise Certificate/PKI service changes
- Design, build, review and implement Akamai WAF, BOT, Site Shield, API web property security configuration changes
- Design, build, review, implement, and administer Palo Alto Prisma CASB solution and policies
- Design, build, review, and implement secure email gateway/mail flow architecture changes
- Design, build, review, and implement automation scripts
- Define regulatory controls and changes
- Define solution hardening standards
- Define secure application development standards

Education and/or Experience:

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree and a minimum seven (7) years of experience working in information security architecture, information security governance, risk and compliance, information security threat and vulnerability management, and/or identity governance and administration; **OR**
2. Information Assurance Management (IAM) **or** Information Assurance Technical (IAT) certifications level 3 plus 5 years' experience.
3. IAM **o**r IAT certification level 2 plus 7 years' experience.
4. IAM **or** IAT certification level 1 plus 9 years' experience.

3. KEY PERSONNEL LABOR CATEGORIES

3.1. Chief Technical Architect (CTA)

The CTA is responsible for providing principles, best practices, innovation, market trends, and future-looking models for the County's IT infrastructure; and serving as a bridge for all the architecture groups and areas as described in Schedule 4.3 for the CTA.

The Contractor CTA works closely with the County's CTA to oversee and coordinate the top-down approach to managing and sharing data, systems, and processes.

Skills and Abilities:

- Exceptional interpersonal skills, including teamwork, facilitation and negotiation.
- Strong leadership skills.
- Analytical and technical skills.
- Written and verbal communication skills.
- Planning and organizational skills.
- Knowledge of all components of holistic enterprise architecture.
- Knowledge of business re-engineering principles and processes.
- Basic knowledge of financial models and budgeting.
- Familiarity with basic graphical modeling approaches, tools and model repositories.
- Familiarity with basic information management practices.
- Exposure to multiple, diverse technologies and processing environments.
- Proven skills and ability to:
    - Participate in the creation or support of the enterprise architecture function/program.
    - Understand, advocate and support the enterprise's IT strategies.
    - Provide analysis of the current IT environment to detect critical deficiencies and recommend solutions for improvement.
    - Provide analysis of technology industry and market trends to determine their potential impact on the enterprise architecture.
    - Balance the long-term ("big picture") and short-term implications of individual decisions.
    - Translate business needs into technical requirements.
    - Estimate the financial impact of technical alternatives.
    - Apply multiple solutions to business problems.

- Leverage existing platforms and services to meet business needs
- Rapidly comprehend the functions and capabilities of new technologies

Education and/or Experience:

Bachelor's degree in computer science, computer engineering, electrical engineering, systems analysis or a related field of study, or equivalent experience. Seven to 10 years of experience in at least two IT disciplines (such as technical architecture, information architecture, enterprise architecture, applications architecture or applications development) in a multi-tiered environment.

3.2. Enterprise Application Architect (EAA)

The EAA is responsible for leading the improvement of application quality, integration, and cost-effectiveness, including reviewing business and technical requirements; assessing, developing and maintaining application standards and architectures; enhancing solution development throughout the project lifecycle; establishing and maintaining data standards, enterprise taxonomies, information management strategies and overall efforts to continuously improve the provision of Services in the EAA's areas of responsibility as described in Schedule 4.3.

The Contractor EAA shall work closely with the County CTA in the governance and oversight of all application development across the enterprise and shall act as a standing member of the Enterprise Architecture Governance Group.

Skills and Abilities:

- Strong knowledge of software development practices and architectures
- Knowledge of information management practices and data architectures
- Knowledge of security-related best practices related to applications and information management
- Proven skills and abilities to:
    - Provide oversight on the design and implementation of cross-functional, multi-platform, and Web-based application systems
    - Provide input into application architecture definition / development
    - Review system design and development processes
    - Provide technical guidance to application development teams and consult on integration and conversion activities
    - Provide guidance and direction on applications portfolio rationalization activities

- Conduct reviews, and analyze organizational needs and goals to develop and implement applications
- Perform high-level entity modeling activities
- Ensure effective software configuration management across applications
- Assesses and effectively manage risks
- Establish and maintain cooperative working relationships between technical and business parties
- Communicate effectively with technical and non-technical users, both in written and verbal form
- Work independently and in a team environment

Education and/or Experience:

Bachelor's or equivalent university degree in management information systems or computer science and a minimum ten (10) years of experience working on software application development projects, of which (3) years must include responsibility for applications architectures.

3.3. Innovation Officer (IO)

The IO is responsible for establish a culture and environment of driving progressive business process change throughout the County. The IO shall be familiar with bimodal approaches to IT and business, skilled in agile and rapid prototyping, strong communications skill to interact with County business and familiarity with innovation and transformation adoption and implementation. The IO shall have experience in developing an innovation charter, rules of engagement for innovation, governance model and success criteria for innovation and continuously improve Innovation Management Services as described in Schedule 4.3.

Skills and Abilities:

- Skilled in seed funding for innovation initiatives
- Natural leadership with excellent verbal/communications skills
- A collaborative working style that moves others to action by planning, motivating and organizing work tasks.
- Strong, demonstrated skills in leading, motivating and supporting staff.
- Extensive program/project management skills.
- Strong personnel management skills.

- Thorough and creative problem solving skills.
- Ability to thrive in a demanding, fast-paced environment requiring a high degree of productivity, adaptability, innovation and follow-through.
- Ability to track and juggle multiple tasks/priorities.
- Self-motivated with ability to work well independently as well as part of a team, and able to provide leadership within that environment.
- Ability to develop and manage budgets and lead and direct others with this responsibility.

Education and/or Experience:

Bachelor's or equivalent university degree in management information systems or computer science and a minimum ten (10) years of experience. A minimum of five years' experience in strategic program development and business model development. Demonstrated public-sector experience in the development and bringing-to-market of programs and services within the context of sustainable business models that both fulfill mission and drive net revenue.

4. NAMED PERSONNEL LABOR CATEGORIES

4.1. Applications Developer – ERP Principal

Applications Developer - ERP Principal serves as the team lead across all ERP architecture domains affected by the interface of one system to another. An Applications Developer - ERP Principal is responsible for evaluating technologies, defining standards, designing and developing solution and reference architectures that solve stated business objectives, in support of ERP interfaces and various custom product enhancements in accordance with standards provided by Oracle.

Applications Developer - ERP Principal is a proficient and effective software developer whose exceptional capabilities and expertise in the ERP domain justifies a premium rate. This labor category will only be used when the tasks that need to be performed require a high level of expertise in ERP applications. It is the combination of the task(s) and individual expertise that justifies the use of this labor category.

For the County's ERP program, this role will:

- Report to the Contractor's Applications Manager
- Interface with the County's Chief ERP Manager to define requirements
- Update Application Implementation Methodology (AIM) MD50, MD 70, etc. technical documents, as needed

- Work with the County to develop new specifications and solutions
- Perform system enhancements/modifications to requirements
- Work with the Contractor's technical team to resolve issues and deliver solutions
- Identify and implement performance improvements

Knowledge, Skills and Abilities:
Knowledge of:

- ERP applications such as EBS, PeopleSoft, Kronos, SAP/Ariba. Ivalua, etc.
- ERP development tools, Forms Designer, Reports, B I Publisher, SQR, etc.
- Design and development of advanced features such as direct upload and download of data files from Application
- In-depth knowledge of the ERP modules and entity modeling
- Fusion Middleware, Service Oriented Architecture (SOA), service buses
- Business process design techniques
- Application design, architecture and development
- Test planning
- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Develop advance script utilities to help team reduce the development time
- Lead the overall design of cross-functional, multi-platform, and web-based data interfaces
- Lead the interface definition, mapping, development, and integration with external applications
- System design and development
- Direct mapping activities on specific technology platforms for ERP Applications
- Provide technical guidance to interface, forms, reports development teams and consults on integration activities
- Conduct reviews and analyzes organizational needs and goals to develop and implement interfaces
- Assess performance, tuning and capacity requirements to determine key technology decision
- Ensure effective software configuration management across applications
- Assess and effectively manage risks associated with their business objectives
- Establish and maintain cooperative working relationships
- Communicate effectively with both technical and non-technical users, both in written and verbal form

- Work independently and in a team environment
- Develop following work products: Interface Design, Create/Update Application Implementation Methodology (AIM) MD50, MD 70, etc., technical documents

Education and/or Experience:
Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree in management information systems or computer science and a minimum eight (10) years of experience working on ERP application development projects, of which (3) years must have been associated with application requirements management; OR
2. Associate degree with two (2) additional years of experience in ERP application development; OR
3. High school diploma with four (4) additional years of experience in ERP application development
4. At least 5 years of experience in ERP application development for large state and local organizations

Restrictions on use:

The use of this Resource Unit (RU) has the following limitations:

1. Limited to the County's ERP program
2. Maximum of two (2) named resources can be assigned to this Labor Category
3. Named resources must be pre-approved by County
4. Roles and responsibilities cannot be transferred to another resource without written County consent

4.2. Electronic Health Records (EHR) Program Manager

The EHR Program Manager is responsible for the Electronic Health Records (EHR) implementation and support services of existing EHR.

The EHR Program Manager shall work directly with the Health and Human Services Agency (HHSA), the Director, IT Services and/or other leader(s) designated by the HHSA Director;

Education and/or Experience:

- Bachelor's degree or equivalent relevant work experience;
- 5+ years of relevant experience in IT program management;
- 3+ years of relevant Health and Human Services domain experience;
- 3+ years of program management of Electronic Health Record solution deployments at large healthcare organizations;

- 3+ years of experience working in health IT supporting hospital and/or clinical operations;
- In addition, the EHR Program Manager preferably should have the following qualifications:
- 7+ years of relevant Health and Human Services domain experience;
- 5+ years of program management of EHR solution deployments at large healthcare organizations;
- 5+ years of experience working in health IT supporting hospital and/or clinical operations; and
- Develops technical program/project management best practices/templates and provide training/mentoring to project teams.

END OF EXHIBIT

Exhibit 16.1-5 – Firm Fixed Price for Applications Maintenance and Operations – Portfolio Applications

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
15Five	15Five is a complete performance management solution to develop your team throughout all stages of the employee lifecycle, from their first day to their last. The more intentional you are with your employee performance strategy now, means less exit interviews in the future.	Yes	HHSA SaaS Support
A&C Captiva Scanning	The County of San Diego (CoSD) /Auditor and Controller (A&C) utilizes a combination of software platforms to capture and store COSD/A&C documents and public records, including data that needs to be kept in perpetuity. Scanning and indexing of this information is done through the Captiva Capture software while retrieval and storage utilize the EMC Application Xtender / File Access Manager product suites. The COSD/A&C utilizes a combination of software platforms to capture and store documents and public records. A&C sites run Captiva Capture and use local scanners to scan and index documents throughout the day. After these documents are scanned, indexed and verified, the index and images are released to the Application Xtender servers (USPLVUCSD075 for index information and USPLVUCSD184 for images).	No	FG3 Full Support
A&C FTP Processes	The federal health and human services departments - Office of Child Support Enforcement (OCSE), will be sending A&C electronic income withholding orders (e-IWO), basically wage garnishment orders, in PDF format. A&C would like these documents deposited into an inbound folder. Once those PDF files are received, A&C staff will review them and provide a response via an acknowledgement on those same PDF files, which will be deposited in an outbound folder for pick up by OCSE using the same SFTP delivery method.	No	FG3 Full Support
AAB Labels	Batch printing of AAB mailing labels & Backup Inquiry.	No	FG3 Full Support
ACAP/ACVV Values, Rates,Apportion	Maintains taxing agency fund values, tax rates, and apportionment ratios. Computes revenue apportionment and allocates to taxing agency funds.	No	FG3 Full Support
Accela Automation (BCMS) (LEAMS)	Accela Automation (BCMS - Business Case Management System) and LEAMS (LUEG Enterprise Asset Management System (go live 4/4/16). LEAMS and BCMS are implemented as separate agencies within Accela Automation.	No	LUEG Full Support
Accounts Receivable and Trust	Manage Receivables&Trust Funds	No	FG3 Full Support
A-Check	A-Check is a DMV approved Employer Pull Notice agent. DHR uses this to monitor employees driving records.	Yes	FG3 SaaS Support
ACL - AuditBond/ Results Manager	Provides a means for the public to confidentially report fraud, abuse and other complaints	Yes	FG3 SaaS Support
ACL Audit Exchange - AuditBond/Results Manager	The ACL - Audit Exchange application provides CoSD with the ability to perform oversight, fraud detection, identify non policy approved use of CoSD issued P-Cards via the running of analytics against P-Card use data.	Yes	FG3 SaaS Support
ACRC Roll Corrections Process	Auditor/Controller PTS Roll Corrections Process - Client-Server - also see PA1047 - Application of changes in property status not identified in prior tax billings	No	FG3 Full Support
ACST/TC Auditor Secured Tax Billing	Auditor system for maintaining Secured Property Tax information	No	FG3 Full Support
ACTI Tax Rate Area Index	Tax Rate Area management system	No	FG3 Full Support
ACUS Auditor Unsecured Prpty Tax Billing	Auditor system for creating tax bills for unsecured properties	No	FG3 Full Support
Administrative Investigations Management	This application is a case management system for the Citizen's Law Enforcement Review Board (CLERB). This application resides in the CITRIX farm and is reached through a shared named "AIM". Problems that the Applications team cannot address will go to the 3rd party COTS Vendor (On Target LLC). HPES' responsibility is to facilitate the vendor's maintenance or upgrade. 3rd party COTS vendor On Target Performance Systems is the leading innovator of human resources software applications and consulting services for Law Enforcement and Corrections. It provides supervisor with the skills and information required to manage employee performance.	No	FG3 Coordinated Support
Adobe Analytics	Web analytics for web site statistics and analysis.	No	FG3 Coordinated Support
Adobe Captivate Prime	External Facing Learning Management System provided by cloud and Adobe systems	Yes	LUEG SaaS Support
Adobe e-Forms APCD Inspections	The objective of this solution is to implement an eForm-based solution for APCD Inspectors to be able to prepare field inspection reports in a highly efficient and accurate manner. The inspectors will be working in an off-line mode without access to the County network. It is necessary to capture digital pictures of violations, include those pictures in the violation report and preserve the high-resolution digital images separate from the violation reports. Data captured in the inspection reports must be transferred to the Accela system when the inspector has access to the County network.	No	Other Full Support
Adobe e-Forms AWM Inspections	The objective of this solution is to implement an eForm-based solution for AWM Inspectors to be able to prepare field inspection reports in a highly efficient and accurate manner. The inspectors will be working in an off-line mode without access to the County network. It is necessary to capture digital pictures of violations, include those pictures in the violation report and preserve the high-resolution digital images separate from the violation reports. Data captured in the inspection reports must be transferred to the Accela system when the inspector has access to the County network. The EDPP LiveCycle technology will be used to implement the project.	No	LUEG Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Adobe e-Forms DEH Inspections	This is an eForm-based solution for DEH CUPA/Hazmat Inspectors to be able to prepare field inspection reports in a highly efficient and accurate manner. The inspectors will be working in an off-line mode without access to the County network. It is necessary to capture digital pictures of violations, include those pictures in the violation report and preserve the high-resolution digital images separate from the violation reports. Data captured in the inspection reports must be transferred to the Accela system when the inspector has access to the County network.	No	LUEG Full Support
Adoptions Assistance Program	End-user maintained application to track aid payments for Childrens' Services, AAP ****Access, PC platform**** End-user maintained application to track Adoption aid payments for Child Welfare Services. This database is used primarily by one person to document new and on-going AAP-eligible clients. Queries and Reports are used to create lists for sending out letters for bi-annual AAP Contract Renewals. Timelines for renewals are to be in compliance with State and Federal law. At any given time, there are over 6, 000 active AAP cases maintained by San Diego County.	No	HHSA Coordinated Support
Adoptions Matching Program	End-user maintained application to match adoption applicants to available children for Children's Services - ****Access, PC platform****	No	HHSA Coordinated Support
Adult Rep (formerly SubPayeePro)	Manages the money for clients that cannot do this for themselves. Funds are deposited into the bank electronically or manually. Bills are paid for clients out of the funds deposited in their "accounts"	Yes	HHSA SaaS Support
Agricultural Preserves	Ag Preserve data base and tracking	No	FG3 Coordinated Support
AIDS Regional Information and Evaluation System	The AIDS Regional Information and Evaluation System (ARIES) was developed by Architier, for the State of California Office of AIDS, the County of San Diego (COSD), the County of San Bernardino, and the State of Texas (the Partners). ARIES will enhance services for clients with HIV by helping Providers automate, plan, manage and report on client data. ARIES will allow the County to provide client level reporting to both State and Federal funding sources. State ASP	No	HHSA Full Support
AIS - IHSS Documentum	This application is an Imaging and content management solution for their AIS In-Home Supportive Services (IHSS) Program with Kofax for the Imaging and Documentum for the Content management system. This implementation will allow Scanning to provide case, client and provider related digital content to be stored into Documentum for the stakeholders.	No	HHSA Full Support
AIS Case Management	Provides content management solution for AIS Case Management Program with Documentum content management system to provide case related digital content stored in Documentum to stakeholders. Key aspects of this application include: • Documentum Integration with AIS Case Management • Scanning and Imaging • Security • Simple user interface • Version management	No	HHSA Full Support
AIS Master Mailing List	Application stored 1200 unique address lists. The Add/Edit Mailing List allows staff to add new people to one or more mailing lists and change addresses. The fields also allow to search for people in the list by name or by organization/agency. The "categories" refer to different mailing lists. By entering "1" in the Category ID box and adding the word "Bulletin" in the Category box, the person is added to the bulletin mailing list. There are several possible numbers linking to a variety of mailing lists. Many of those lists are not used, but could be restarted. Only about 3-4 categories are used now. Staff can also make a mail merge of people in certain categories as well. Regularly, labels are printed from this software for either the bulletin or the Safe Seniors newsletter. Staff also has a Zip code account to help with cost of mailing, as the labels are presorted by Zip code	No	HHSA Full Support
AIS Ombudsman	Provides a content management solution for AIS Ombudsman Program with Documentum content management system to provide volunteer, complaint and facility related digital content stored in Documentum to stakeholders.	No	HHSA Full Support
AIS-IHSS Kofax Imaging	Electronic Content Management (ECM) system for scanning, storing, and retrieving IHSS case files	No	HHSA Full Support
AlertSanDiego	Blackboard Connect (aka AlertSanDiego) is the region's emergency mass notification system. The system allows authorized users (County, cities, special districts) to conduct external (i.e. public alert and warning) and internal (i.e. notifications) to recipients via voice, email, and text message. The system contains all listed and unlisted landline phone numbers (E-911 data), AlertSanDiego registrants, and internal notification lists (e.g. EOC activation lists and staff notification callouts). This program enhances the regions ability to communicate with the public and provide timely emergency information in the event of a disaster.	Yes	PSG SaaS Support
ALEX	AIS provides services to older adults, people with disabilities and their family members, to help keep clients safely in their homes, promote healthy and vital living, and publicize positive contributions made by older adults and persons with disabilities. AIS has more than 30 programs and provides a wide range of services, including information and assistance, advocacy, coordination, assessment, and authorization of direct services. ALEX supports the referral intake and processing for these programs: IHSS, MSSP, SOAR, Linkages, APS, ST, I and A.	No	HHSA Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
AlinIQ Inventory Management System (IMS)	Web based Laboratory Inventory Management System installed in the San Diego County Public Health Laboratory on Rosecrans.	No	HHSA Coordinated Support
Alzheimer's Project AEM Website (SDAlzheimersProject.org)	Alzheimer's Project AEM website on Adobe Experience Manager (AEM) platform.	No	HHSA Full Support
Amazon Web Services (AWS) EC2 GovCloud	Amazon Web Services Elastic Cloud Computing (AWS EC2) GovCloud is a tool to quickly analyze, optimize, and discard unneeded IT solutions. Outcome is to reduce agency spending, reduce time to implementation, and to have a better understanding of a solution prior to any further spending or committments.	Yes	HHSA SaaS Support
American Legal Code Codification	The contractor publishes the County of San Diego Administrative Code and the County of San Diego Regulatory Code in print, on CD-ROM and on the Internet. The contractor accepts the Codes in Folio Views CD-ROM format and maintains an Internet site containing both the Administrative Code and County Code of Regulatory Ordinances. The Internet site is made available to the public at no charge to the users and allows the public to search the Administrative and Regulatory codes. The contractor updates the Internet site within five days of receiving updates from the County. The contractor also offers hard copies and CD-ROM copies of each complete Code and subscriptions to a monthly update service. In the 1990s, the Clerk of the Board outsourced its production and distribution of the Countys Administrative and Regulatory codes. Since 2000, the County has made the Administrative and Regulatory codes available online for the public and internal staff through an outside contractor. The contractor provides this service based on Purchasing & Contracting Request for Bids (RFB) NO. 5453. It is cost efficient to use the same contractor for online code publishing that provides hard copy updates to the Administrative and Regulatory codes.	Yes	FG3 SaaS Support
Animal Control - Lost and Found/Pet Adoptions	Web Application for Animal Control Lost and Found and Pet Adoption.	No	PSG Full Support
AP Invoice Imaging System	Accounts Payable Invoice Imaging System (APIIS). APIIS is based on the Electronic Data Processing Platform (EDPP). EDPP is PA2563. The Accounts Payable Invoice Imaging System (APIIS) is a replacement for the County of San Diego's XenDocs Imaging System, which serves as the repository for scanned Accounts Payable invoice-related documents and enables County of San Diego (CoSD) staff to search, view and manage those scanned documents. APIIS will provide new features and functionality to enable the County to streamline AP Invoice processes, in addition to functionality currently provided by the XenDocs Imaging System. As such, the County will be able to maintain its core Accounts Payable Invoice document processes, and to continue utilizing its established base of over one-hundred PC workstations distributed throughout the County, at approximately fifty-three department sites. As the new replacement for the XenDocs Imaging System, APIIS will define the way in which the scanned AP documents are organized, stored and managed for the Oracle Accounts Payable (AP) module of the CoSD's Oracle E-Business Suite (EBS).	No	FG3 Full Support
APCD - OpenGov	Budgeting, planning, and projections system	Yes	Other SaaS Support
Applications Manager	Applications Manager (AppsMgr) is a web-based tool used to track and report on portfolio (PAID) applications, cloud (CAID) applications, infrastructure applications (IAID) and desktop applications (DAID). Each application can be associated with Servers that it uses, the Software products it uses, and the relevant MSIs, and Contacts such as the vendor, owner, and primary support contact. Reports can be generated onscreen or exported to Excel. Requests for new portfolio applications are initiated in AppsMgr and get assigned a unique PAID by the AppsMgr administrator. Additionally, application changes are submitted to the AppsMgr administrator for approval. Approved changes are logged in the Change Log and included in the CoSD Portfolio Applications Catalog. Additionally, the application displays information on Cloud applications and its' contacts which is populated and updated via a scheduled task.	No	ITO ITO Owned Support
APS Imaging	The Documentum web based application which allows the scanning, indexing, and retrieval of documents. Document are imported into the Documentum system and placed in the appropriate folders with the appropriate security. Webtop is using to retrieve the documents.	No	HHSA Coordinated Support
ARCC Captiva Scanning Solution	The ARCC Captiva Scanning Solution is utilized for scanning Prop 8 Assessment requests and other department capture needs.	No	FG3 Full Support
ARCC E-Commerce	ARCC e-commerce	No	FG3 Full Support
ARCC Intranet Applications	Public access to PCs for Assessor Maps for a fee	No	FG3 Full Support
ARCC Mills Act DB	Tracks Mills Act exempt property	No	FG3 Coordinated Support
ARCC SharePoint Site	The ARCC Department has implemented a SharePoint Environment that supports both Intranet and Internet access. Support is performed by the Peraton SharePoint Team. Note: Patching to this app requires that the database be taken out of high availability mode.	No	FG3 Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
ARCCs AX/WX/WFM Applications	Applicationxtender (AX), Webxtender (WX), and Workflow Manager (WFM) are software components from the EMC Documentum ApplicationXtender Product Suite used by the ARCC for their "Imaging" applications. The Workflow Manager component allows them to implement "workflow process" to their image capture procedures. NOTE: ApplicationXtender and WebXtender are used by other business groups in the County.	No	FG3 Full Support
ArcGIS Online	Online mapping and data services	Yes	LUEG SaaS Support
Archive-It	The service will be used to capture and archive public ARCC webpages.	Yes	FG3 SaaS Support
Articulate 360	Articulate 360 is a cloud based application that allows users to develop and publish educational content for distributed use. This application will be used to provide educational programs for Parks and Recreation managed natural resources.	Yes	LUEG SaaS Support
ASAD Secured Prpty Assess Info System	Assessor Secured Property Assessment online/Database management system	No	FG3 Full Support
ASAPnet Desktop	This is a project to provide desktop computing, printing, and collaboration to Reserve Firefighters (non-County employees) remotely located at County fire stations.	Yes	PSG SaaS Support
ASAS Secured Prpty Assess Ownership&Valu	Assessor Secured Property Ownership and Valuation management system (Includes Prop 58 System)	No	FG3 Full Support
ASPA Supplemental Property System	Secured property supplemental assessment management system	No	FG3 Full Support
ASRC Roll Corrections Process	Assessor Roll Corrections Process - MF with Client-Server DB - also see PA1017 - Application of changes in property status not identified in prior tax billings Configuration & installation docs tied to PA1017	No	FG3 Full Support
Assessment Appeals Board System	Tracking/scheduling of Appeals	No	FG3 Full Support
Athena IDX	Managed Care Application for CMS Program. The application is an Linux hosted application that is accessed through the Web. The Web is set up on window servers (test & prod) The URL on the window servers accesses the application and associated database which run on Linux servers (test & prod). The application also includes a module that utilizes the sFTP server for retrieving data from UHC (UHC interface) and NetChemistry (AuthMed interface) for use in the IDX application.	No	HHSA Full Support
Auditor & Controller Managed Forms	This solution includes the implementation of Adobe PDF e-Forms for the Auditor & Controller (A&C) Department. County Users will view and fill-out the forms using Adobe Acrobat 2017 or higher. The A&C Information Technology Management Services group will be responsible for publishing the PDF e-Forms in the "Forms" section of their departmental SharePoint site (i.e. County's "InSite").	No	FG3 Full Support
AutoCAD	AutoCad Civil 3D Network This Server can not be Refreshed or migrated unless the Name and MAC number are the same on the New Server.	No	LUEG Coordinated Support
Autocad	Tool used to create maps	No	FG3 Coordinated Support
AutoCAD Raster Design	Autocad integrated tool	No	FG3 Coordinated Support
AutoLISP Files	CAD customization language environment	No	FG3 Coordinated Support
Automated Import tool for Performance Review	Performance Appraisal forms are verified and imported. The overall business imperative is to verify that Performance Appraisals are submitted in a timely manner and according to policy and that they are imported to the correct Employee folder in Documentum. Provide controls to ensure the accuracy of both the information on the Performance Appraisal form and the importation into Documentum.	No	FG3 Coordinated Support
AXAddOns	The AXAddOns application is a set of Macros/Utilities installed on client workstations to facilitate their interaction with AX applications. Special Awareness Application Script - Extra macros, schemes, and keyboard mappings files required for ARCC Applications XTender	No	FG3 Coordinated Support
Axcelerate eDiscovery	The Axcelerate eDiscovery application is used to automate the e-discovery process. Uses digital forms of documents.	No	FG3 Coordinated Support
Beach and Water Quality (BWQ)	Beach and bay sampling is currently being conducted by Department of Environmental Health (DEH) at 78 beaches across San Diego County. The Board of Supervisors have directed LEUG to update the beach and bay monitoring page (http://www.sdcounty.ca.gov/deh/water/beach_bay.html) to provide beach water quality data that is easier to access and understand by delivering it in a format that supports multiple device types and formats (i.e., "how they want it" and "when they wants it").	No	LUEG Full Support
BHS Emergency Rental Assistance Program	This application assists with the provisioning of housing funds for Covid19 housing eviction relief. It is also known as ERAP for short. The application was created and will be supported by Basc LLC and hosted on AWS. A similar application was created for for Housing and Community Development Services. It includes a secure website with modules for applicants and administration staff which will be accessible via internet and mobile devices (including smart phones and tablets).	No	HHSA Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
BHS Financial Management System	BOARD Cloud is a SaaS version of the BOARD all-in-one platform, which allows one to analyze, plan, simulate and forecast. It is designed to offer seamless connection to cloud data systems in real time. BOARD Cloud allows you to deliver enterprise analytics, planning and forecasting that fully leverages existing software investments.	No	HHSA Coordinated Support
Bitly	Established in 2008, Bitly is a URL shortening service and a link management platform. It is privately held and based in New York City, with offices in Denver and San Francisco. Bitly shortens 600 million links per month for use in social networking, SMS, and email.	Yes	PSG SaaS Support
BlackLegacyNowSD.com	The BlackLegacyNow site provides education, multiple resources, and awareness of African-American infant mortality and preterm birth to the public. Additionally, it is a source for the public to connect to the San Diego County Perinatal Equity Initiative (PEI) program.	Yes	HHSA SaaS Support
B-Link	Fraud Referral system This is a Microsoft Dynamic 365 Cloud application that will be BPAI's case management system replacing their current FRTS, PTS and Hotline applications. The application will integrate with CALWIN, CMIPS, and EDPP.	No	PSG Full Support
Bluehost.com Website Hosting	Bluehost is a web hosting solutions company. They provide comprehensive tools to millions of users throughout the world so anyone, novice or pro, can get on the web and thrive with their web hosting packages.	Yes	HHSA SaaS Support
BlueJeans	This system will provide the San Diego Urban Area emergency managers with the ability to communicate emergency incident information utilizing a cloud based web conferencing service that can be accessed using a variety of types of devices and network connections. This flexibility is a critical capability when attempting to communicate accross multiple jurisdictions with a variety of methods. The service will include video, voice and web conferencing capabilities. This capability will provide a tool to support effective interagency communication of information in the San Diego Urban Area.	Yes	PSG SaaS Support
BMC Footprints	Service Desk Management Software used by Operational Support HelpDesk, HHSA. BMC FootPrints is a flexible, comprehensive, integrated IT service and asset management platform that is easy to install, use, and extend to create business value. BMC FootPrints is a web-based, on-premise solution that is quick to install and easy to use.	No	HHSA Full Support
BMI DR 6.1	Allows staff & the public to view historical documents, Land records, miscellaneous and official records through 1989.	Yes	FG3 SaaS Support
BOS District Five Website (AEM)	WWW County Web Site (split out from PA1777)	No	FG3 Full Support
BOS District Four Website (AEM)	WWW County Web Site for Board of Supervisor representing District 4	No	FG3 Full Support
BOS District One Website (AEM)	BOS District One Website for www.supervisornoravargas.com	No	FG3 Full Support
BOS District Three Website (AEM)	District 3 AEM hosted website	No	FG3 Full Support
BOS District Two Website (AEM)	WWW County Web Site	No	FG3 Full Support
BrightSign	The BrightSign Network is an affordable and scalable subscription-based hosted service, providing the complete infrastructure to serve and support a digital signage network. It stores and delivers remote content to one or many units.	Yes	LUEG SaaS Support
Brown Armstrong	Brown and Armstrong will provide annual audit and review services for 1) The County Investment Pool and its financial statements2) Investment policy compliance	Yes	FG3 SaaS Support
Budget Books	The Budget Books Application provides a means for the County to store historical financial documents. In 2014 PA2447 Budget Books was migrated to EDPP and now resides in the COSDGEN Repository. Budget Books contain budget documentation dating back to the 1928-1929 fiscal years. This PAID has the following traits: • No association with any other application • Users access the repository via CARA • At one time, documents were imported via Kofax Ascent Capture • Documents prior to 1998 were imported in TIFF format. In 2009, Wave TSG was contracted to provide PDF +Text Rendition and Versioning for all documents in the Budget Books Cabinet. • The department no longer scans or imports documents to this repository. Budget Books is used primarily for historical research. The last folder created was for the 2009-10 Fiscal year. • The Budget Books Cabinet is configured for full text indexing so that it can be used with Xplore for integrated searching. • No retention policies have been configured. However, these documents are historical and therefore must conform to the "Permanent" retention policy. • No customizations have been provided. For specific information on Users, Groups, and ACLs, please refer to either the Solution Design or Migration Specification Documents within DocVault.	No	FG3 Full Support
Building Automation System (BAS)	This application allows for the Tridium devices (JACEs) to send data. JACEs collect the data from the different building control systems like HVAC, etc and then send the data to the NiagaraAX software installed on the VM server.	No	FG3 Coordinated Support
Business Audit Tracking	Audit tracking for Assessor Business Division	No	FG3 Coordinated Support
Buynet II	Web based purchasing tool	No	FG3 Full Support
CAL FIRE CAD2CAD	This application is used by CoSD "CAL FIRE" to coordinate and track Fire Vehicles and Resources across appropriate locations and interface with the State systems.	No	PSG Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Calameo	Calameo is an easy document sharing and publishing service that lets you create online magazines from your offline documents. You could upload PDF files, spreadsheets, word documents and powerpoint presentations to create reports, magazines, catalogs, brochures etc and publish it online. Once published, it can be easily shared across multiple social networks, emailed to customers and added to the community where you can get feedback from readers on the published material.	Yes	LUEG SaaS Support
California Medical Services NET	CMSNET is a cat 2 Client/Server application. The server and the application are maintained by State CMSNet Help Desk (Brian); CMSHELP@DHS.CA.GOV 866-685-8449	No	HHSA Coordinated Support
CalWIN	The entire integrated system comprised of and connecting all CalWIN System Software, Local Office Hardware, Project Facilities Hardware, and Third Party Software licensed by COUNTIES or licensed by VENDOR. This is an ASP application hosted by the CALWIN project. ASP is a language similar to VBScript developed by Microsoft. ASP is included and supported by IIS (included with Windows Server).	No	HHSA Full Support
CalWIN CERMS	This is a Documentum Application, used by County Eligibility Staff to retrieve, view, store and modify eligibility forms and client documents. This is the replacement of the old DoRES application. CERMS ACS Project - The objective of this project is to utilize the USPS Address Correction Service (ACS) to receive electronic nixie notifications from the USPS in lieu of having the physical mail pieces returned. The electronic nixie notifications would be used ot automatically generate synthetic documents that contain all relevant information about undeliverable mail pieces. Those synthetic documents would be automatically stored in CERMS and would be processed by the WMS.	No	HHSA Full Support
CalWIN CIS Data Mart	CIS database for CalWIN	No	HHSA Full Support
CALWIN Interfaces - no interactive login	This PAID consists of the interface pieces of Calwin PA2241. A few of the interfaces call an application called Transform(PA2605) which reformats the printed warrants with County of San Diego specific requirements (Series 27, 28, 29). Other interfaces included in PA2344 are things such as “Positive Pay”, “Direct Deposit”, “CalHEERs”, “Collections”, “Childsupport”, etc.	No	HHSA Full Support
CampaignDocs.net	Keeps track of candidate filing information/disclosure statements. Allows candidates to file for office on line. Data in this system is open to the public, and most data is available to the public via web browser, however there are specific additional regulations governing the release of some of the data	Yes	FG3 SaaS Support
Candidate & Measure Portal	SaaS solution to enable submissions of Candidate Statements, measure text and any other measure content that need to be collected by the ROV for each election cycle. The objective is to reduce the task of scanning, cutting and pasting from hard copy submission or word docs into a template for ROV.	Yes	FG3 SaaS Support
Cantata Health Netsolutions	NetSolutions vendor is now Experience Care. Primary clinical medical record system including MDS, Resident Trust and medical billing. It includes Physicians Orders, eDocuments, ePrescribing, Progress Notes, Quality Assurance, User Defined Assessment, Tracks resident information, including census, reimbursement, clinical, and contact data. NetSolutions also contains AR/billing software, beginning with complete registration data, continuing to claims paid on first submission Hospital for medical billing to Medicare & Medi-Cal.	No	HHSA Coordinated Support
Canva	Canva is a graphic design tool with extensive templates, graphics, color pallettes, and other design elements. It allows templates and branding to be established, and promotes collaborative development of materials.	Yes	FG3 SaaS Support
CapitolTrack	This application is used by S&IA to track State Bills that are introduced and amended during the California legislative session.	Yes	FG3 SaaS Support
CAR	CAR is a Microsoft Access application used by the County of San Diego Department of human Resources to maintain Classification Activity Requests. DHR users access the application using the Citrix remote access solution.	No	FG3 Full Support
Card Access System (CAMS)	CAMS (Access Management) has a web based application for access management control. The web interface allows maintenance of employee data and access history. CAMS (Access Management) also has a workstation component which creates and prints the access badges. The badge printing is managed from several locations to provide independent badge control at the departmental level; each location prints unique badges that can only be used at that location – the exception being General Services who manages all county-wide badges excluding the restricted departments. Locations include: the Department of General Services, the District Attorney’s Office, the Sheriff’s Department, the Courts and the Probation Department	No	FG3 Coordinated Support
Case Review System	Supervisor and QA Review of Cases	No	HHSA Coordinated Support
CDPH External Connect Gateway (ECG) Quick Connect	External Connect Gateway (ECG) Quick Connect (QC) is the California Department of Public Health's (CDPH) web portal solution that provides a secure means of transmitting daily COVID-19 case data from CoSD to the state.	Yes	HHSA SaaS Support
CECRIS	CECRIS is a CDSS information system development project with the primary goal of: [1] Providing a single integrated system that supports end-to-end processing of the CEC and CA 800 processes to fully meet the business needs; [2] Creating a flexible and expandable system to accommodate federal and state mandated modifications and reporting requirements; [2] Complying with federal and state program guidelines and standard accounting principles; and [4] Comply with state IT and security standards.	Yes	HHSA SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Central Replay System	Compliance regulations require HHSA to maintain legacy call recordings, storage, and playback for a period of 10 years. Avaya's Central Replay System (CRS) provides HHSA with the ability to store recordings indefinitely and access the recordings as needed. No new recordings will be added via this solution.	No	HHSA Coordinated Support
Cerner CareTracker – On Premise	CareTracker application uses wall-mounted touch screen devices placed strategically throughout Edgemoor Hospital to allow staff members to record supportive documentation of all types. Information for all departments is retrieved in a variety of formats for MDS completion, care planning, and staff management. The Application consists of 3 programs, the main CareTracker Application, the QlikView publishing server and a QlikView web server for viewing the QlokView data. Each of the server runs Windows server and access a database server running SQL Server on Windows Server. The kiosks communicate with the server via two appliances (computers) located in the phone closet at Edgemoor hospital that act as a FIFO buffer between the kiosks and the server. 11/02/21 - Application PA2561 is used 24/7. All maintenance windows must be coordinated in advance with customer.	No	HHSA Coordinated Support
Cerner RHO	Cerner RHO is a suite of applications offered by the vendor Cerner Corporation (http://www.cerner.com/public/) and is used at the San Diego County Psychiatric Hospital (SDCPH) and Inpatient and Outpatient pharmacies. PA2732-Cerner RHO includes Millennium RHO and Cerner Retail Pharmacy RHO. Millennium RHO is accessed by hospital clerical staff, doctors, nurses and pharmacists to track patient information, chart patient data, and dispense medication. At the Inpatient Pharmacy and hospital there are 4 Rx stations that dispense drugs, one in each unit, Units A (EPU), B, C and D, and 5 label (Zebra) printers, one in each unit and one in the pharmacy to print lab specimen labels and prescription labels. Special printers for the wristbands worn by patents and barcode scanners for the patient wristbands, wireless vitals monitoring instruments and wireless iPods and iPads for use in charting patient data, and large wall mounted touchscreen computers in each unit to display patient information for the patients in each unit. Cerner Retail Pharmacy RHO is used by the Outpatient pharmacy to dispense medications to county residents who are NOT inpatients of the San Diego County Psychiatric Hospital (SDCPH). Cerner Retail Pharmacy RHO utilizes standard laser printers to print prescription labels and uses scanners to scan prescriptions and signature pads for patients to sign for the receipt of prescriptions.	No	HHSA Coordinated Support
Chameleon	Animal Management: Chameleon is an integrated shelter software case management system for the entire Animal Services agency. It helps to track all the data for shelter, law enforcement, licensing and dispatch programs within the department. Finding Rover. Finding Rover is a Third Party Mobile App that uses Animal Facial Recognition against the Picture data provide from the Animal Database. AP Refund. Autosys runs the AP refund application monthly (25th of each month). It uses the FTP server COSDI022P to transfer the files to. the Oracle Financial System for processing.	No	PSG Full Support
ChargePoint	Infrastructure to enable County electric vehicles to charge battery.	Yes	FG3 SaaS Support
Child Health and Disability Program/Children Youth and Families/Health Care Program for Children in Foster Care	Expansion of HCPCFC Public Health Nurse Web-Enabled Statistical Reporting System. Child Health and Disability Program/Children Youth and Families/Health Care Program for Children in Foster Care. This is an ASP application hosted on the web server with other applications. ASP is a language, similar to VBScript, developed by Microsoft. ASP is included and supported by IIS (included with Windows Server). The application was developed by Rushmore Group LLC (http://www.rushmore-group.com/).	No	HHSA Full Support
Choosewellsandiego.org	Choosewellsandiego.org is a website that is designed to provide information for caretakers of individuals who need assisted living. The choosewellsandiego.org site includes a seach feature that offers a rating system for residential care facilities for the elderly (RCFEs) in San Diego County to provide the public with accessible information needed to differentiate quality facilities from substandard ones and links to other resources related to long term care.	Yes	HHSA SaaS Support
Chronic Disease Surveillance	The Chronic Disease Surveillance Database collects Public Health and Chronic Disease data for the Chronic Disease and Health Equity Unit of HHSA. The data is analyzed to identify the prevalence of diabetes, heart disease, and stroke, and associated conditions in San Diego County. The application uses SharePoint, https://sdcountycagov.sharepoint.com/sites/HHSA-CHRONDIS/SitePages/Home.aspx, for receiving data from contributors. Contributors upload a file containing the data, in the format specified in the SDD, and the application processed the file and adds the data to the database.	No	HHSA Full Support
Citizen Advisory Boards Application	Clerk of the Board Commissions and Boards Application. Tracks applicants and members of county boards and commissions.	No	FG3 Full Support
CityWorks	Asset management system for WasteWater Division	Yes	LUEG SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
ClaimRemedi	ClaimRemedi is a SaaS solution that provides HHSA ability to submit electronic medical bills/claims, for BHS, Edgmoor and PHS, to payers such as insurance providers, Medical, Medicaid, Medicare, etc.	Yes	HHSA SaaS Support
Clarity	Clarity is the Homeless Management Information System used by the San Diego (Continuum of Care) CoC to capture and report on client, project, and system level information regarding homeless services utilization, performance, and outcomes. It may only be accessed by persons who have been pre-approved by Regional Task Force on the Homeless (RTFH) and are either completing or have successfully completed Clarity training.	Yes	HHSA SaaS Support
ClassMarker	ClassMarker is a professional, easy-to-use online testing system, that allows you to create your own tests, in minutes. Because ClassMarker is online, there's no software installations for you or your users, so tests can be taken instantly. Founded in 2006.	Yes	HHSA SaaS Support
Clear Impact	Clear Impact Scorecard is an online, web-based software tool that will provide, implement and support a performance management system that supports shared measurement, comparative performance, and adaptive learning.	Yes	HHSA SaaS Support
Closed Cases Repayment Accting System (CCRAS)	Repayments on Closed Cases from CDS legacy system	No	HHSA Full Support
CME Web	Case Management System for Medical Examiner Application is owned by the Medical Examiner's office. Application is a critical database for CoSD Medical Examiner's office which functions as a case management system. CME Infrastructure, Server Name, Domain Names, IP addresses, and Software Version installed are documented on the HP "SCM" Configuration Management system. The Medical Examiner's office access this application via the web links listed below. There are no external users/customers. The Web based application resides on an IIS server accessing a MS SQL database. There is a TEST and PROD environment. Clients access this application via Web Browser (Chrome)	No	PSG Full Support
CMIPS Adhoc Tool	CALIF MGMT & INFO PAYROLL SYS - Monthly reporting & loading of CMIPS II data to the CMIPS Adhoc tool.	No	HHSA Coordinated Support
CMIPS II - State Hosted	Case Management Information and Payrolling System (CMIPS) is an information computer system that tracks more than 300,000 cases and processes over $2,000,000,000 annually for state-wide services provided to elderly, disabled, or blind individuals so that they can remain safely in their own homes under the In-Home Supportive Services (IHSS) Program. CMIPS II is a State hosted Application and is accessed through a Web Portal that provides a single log-on location for HHSA IHSS Program users to access the various components and functionality associated with CMIPS II. These components and functionality include Case Management, Reporting, Advantage Financial and Advantage Human Resource Management (HRM). CMIPS II is an upgrade/enhanced Application from the Legacy CMIPS Application.	No	HHSA Coordinated Support
CMS Patient Eligibility System	This is a patient eligibility system. As of 06/30/2014, the application will be hosted at NetChemistry's site.	No	HHSA Full Support
CMSNet iQIES	Edgemoor is a licensed skilled nursing facility regulated by the California Department of Public Health (CDPH) and receives federal funding based on compliance with Centers for Medicare/Medicaid Services (CMS) requirements. Edgemoor's administrative team (approximately 10 users) use CMSNet to submit direct care staffing information and other nursing home data based on payroll and other auditable data to the Centers for Medicare and Medicaid Services (CMS). The data submission is done electronically by accessing the CMS site via Pulse Secure.	Yes	HHSA SaaS Support
COB Public Search	Clerk of the Board's Documentum Document Management System. This application is mainly used by the Clerk of the Board staff to view Agenda documents, Board Letter Documents, Minute Order documents and other Supporting documents which was created in Legistar application. Clerk of the Board Staff members create these documents in Legistar/Granicus application and the sync job integrates with Granicus API and upload the documents from Legistar/Granicus to Documentum repository. Also the staff create Communications Received documents and RTS records using this system. This application also have 2 public components. 1) Agenda Calendar 2) Public Search These components are used by public for searching Board Letters, Agenda documents, Minute Orders and Supporting documents.	No	FG3 Full Support
CobbleStone Data Synchronization	The CobbleStone Systems Database Synchronization Module is designed to back up the files that are imported into Contract Insight and store them onto a local computer. The files are copied daily to a desktop..	No	HHSA Coordinated Support
Columbia Ultimate RPCS	Columbia Ulitmate RPCS - AIX	No	FG3 Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Community Enhancement / Neighborhood Reinvestment Program (AC Grant)	The CE/NRP application is used throughout the year by the Office of Financial Planning (OFP), Clerk of the Board (COB) and the Board of Supervisors (BOS) to manage the lifecycle of financial grants awarded to public entities by the BOS. Specifically, CE/NRP accepts grant applications via provided Adobe forms, then awards, tracks, closes and stores successful award data in its database over multiple years. This application is built upon the Enterprise Document Processing Platform (EDPP). EDPP is PA2563. The ACGrant system is comprised of a database, a web front end and a web service. The database runs on Microsoft SQL Server and the web components run on Internet Information Server (IIS). Both the database and web servers run on the Windows Server operating system. In addition, a component called Documentum processes grant applications submitted electronically (via PDF files) and submits the applications to ACGrant.	No	FG3 Full Support
Community Grants Application	The Community Grant program established by the Board of Supervisors is built on the model created by the COVID-19 Small Business Stimulus Grant Portal. The Community Grant application will be used throughout the year by the Office of Financial Planning (OFP), and the Board of Supervisors (BOS) to manage the lifecycle of financial grants awarded to public entities by the BOS. Specifically, the Community Grants portal accepts grant applications via provided Adobe AEM web forms, then awards, tracks, closes and stores successful award data in its database over multiple years.	No	FG3 Full Support
Community Resource Directory	The Probation Department seeks to host a newly developed and acquired application known as, the Community Resource Directory (CRD) application within the HP/CoSD environment. This application was developed by Clear Wave Software and will be used to match probationers with care and programs within their community.	No	PSG Coordinated Support
Comparable Sales System	Real estate comp sales	No	FG3 Full Support
Comprehensive Access Tracking (CAT)	16355 - Revenue & Recovery – Administration	No	FG3 Full Support
Constant Contact	Constant Contact is an online subscription web service that provides the library with the ability to send e-newsletters to customers.This subscription service is voluntary for customers they sign up to receive the e-newsletters by providing their email address. Customers can unsubscribe at any time. The service does not collect customer names or any other information. This subscription service does not communicate with the librarys integrated library system (ILS).	Yes	LUEG SaaS Support
Contact Wireless TXTPAGE plus	Contact Wireless provides a SAAS solution allowing for bulk and instant text messaging with DCSS customers who will opt in to receiving text messages. The software allows a DCSS employee to utilize their internet connected pc into a text capable cell phone sending texts via the TXTPAGE plus website.	Yes	PSG SaaS Support
Contract Insight	Used by HHSA to manage a contract portfolio of over 900 contracts with a value over $400 million. This database & workflow system is used by HHSA to manage contract information as well as the contracting processes, including procurement tracking, contract administration, and monitoring.	Yes	HHSA SaaS Support
Contract Lifecycle Management (CLMS)	Applications allows for tracking and managing procurement of supplies and equipment and provide for suppliers to have open bidding for supply requests. This is a new application being procured and implemented for the management of contracts within the County of San Diego.	No	FG3 Coordinated Support
Contrail	The San Diego County Flood Control District (FCD) needs to upgrade its flood warning software to accommodate a new radio protocol being instituted industry-wide to improve efficiency of the use of the radio spectrum. A new, more efficient radio protocol, called ALERT2, was developed and vendors have responded with new software and hardware.	Yes	LUEG SaaS Support
Convey 1099	This application is used by Fiscal to enter and manage CY 1099 database to be sent to IRS. Use to prepare the TIN Matching file to IRS and print the 1099Misc . Application is updated yearly in January for prior tax reporting year.	No	HHSA Coordinated Support
CoSD COVID-19 Emergency Rental Assistance Program 2021	This application consists of 2 Web portals in response to COVID-19 housing eviction relief. It was patterned after the HHSA HCDS ERAP application, PA2804 and HHSA BHS application, PA2813. There are modules for applicants and administration staff, a decisioning for eligibility logic and a randomization & lottery function for all applicants. The application was created and will be supported by Basc LLC and hosted on Perspecta AWS.	No	HHSA Full Support
CoSign Digital Signature	CoSign Digital Signature will allow users to digitally sign documents. This is enterprise wide and includes Sheriff and DA.	No	FG3 Coordinated Support
CoStar Comps	CoStar conducts expansive, ongoing research to produce and maintain the largest and most comprehensive database of commercial real estate information. Our suite of online services enables clients to analyze, interpret and gain unmatched insight on commercial property values, market conditions and current availabilities. Headquartered in Washington, DC, CoStar maintains offices throughout the U.S. and in Europe with a staff of approximately 1,500 worldwide, including the industry's largest professional research organization.	No	FG3 Coordinated Support
County Constituent Relationship Management	Constituent Relationship Management for tracking constituents and public referrals	No	FG3 Full Support
County EMS P&P	EMS Application for Protocols, Processes, and Procedures	No	PSG Full Support
County Internet Website (AEM)	Enterprise Web Solutions platform, which includes all AEM (Adobe Experience Manager) Websites.	No	FG3 Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
County Intranet Site	SharePoint Insite - This site is the internal County Intranet SharePoint website for group and department employee information. The primary path for all county, Sheriff and DA users is via https://sdcountycagov.sharepoint.com/sites/InSite/Pages/default.aspx. This PAID has absorbed the functionality of PA1855 (Phone Directory). Major update to include Powell implementation of Synergy.	No	FG3 Full Support
County Law	Case tracking, calendaring, and timekeeping system for County Counsel cases	No	FG3 Coordinated Support
County Library Website	7/2021: The SDCL.org website moved off of the AEM infrastructure to a SAAS vendor solution.	No	LUEG Full Support
County Web Mapping Applications	PA2005 County Web Mapping Application contains the County intranet/internt map sites implemented with the County of San Diego's Internet Mapping Service framework.	No	LUEG Full Support
COVID-19 Lodging	This app is written in Power Apps and records cases for COVID-19 patients and allows the call agent to assign these patients to a hotel/motel lodging for 2-week isolation if they are unable to self-isolate at home.	No	HHSA Full Support
CPA Fringe Benefits Processing	Fringe benefit tracking systems that allows the County department users to complete and approve an eForm that will be extracted and managed in a CARA viewer.	No	FG3 Full Support
CrisisTrack	LUEG Damage Assessment & Disaster Recovery	No	LUEG Coordinated Support
CRM2016 Framework HHSA	CRM Framework HHSA	No	HHSA Full Support
CSE-IT	Commercial Sexual Exploitation-Identification Tool (CSE-IT) is a checklist of indicators that helps the service provider integrate information routinely collected in practice into one document that does not change the interaction between the service provider and the youth, but helps the provider to think about the information routinely gathered in their practice in the context of exploitation.	Yes	HHSA SaaS Support
Cut Log Tracking	Track parcel cuts	No	FG3 Full Support
CWS / CMS (State ASP)	Childrens Services Client database, Perspecta supports application for front end connectivity to CWS/CMS database/State maintains back end database	No	HHSA Coordinated Support
CWS Folder Control and SSRS Archive	This is a Microsoft Dynamic 365 Cloud application that is used for Child Welfare Service (CWS) Folder Tracking and Social Service Reporting System (SSRS).	No	HHSA Full Support
CWS Mandated Reporter	The Child Welfare Services (CWS) Mandated Reporter Application (MRA Web) is a web site used by CWS social workers and community Mandated Reporters to submit/receive the follow up Suspected Child Abuse Report (SS8572). As a Mandated Reporter calls the child abuse hotline to report a suspected child abuse, the social worker uses the application to generate initial follow up report and ensures that a login credential exist for the Mandated Reporter. The Mandated Reporter completes (submits) the generated follow up report online and in a secure manner. Along with the follow up report, the application allows for the uploading of supporting documents. Once submitted, the application enables the social workers and the Mandated Reporters to search for and view/print the report and the supporting documents.	No	HHSA Full Support
CWS Ombudsman	This application is used to collect information on all Fatalities/Near Fatalities, client escalations, contacts, issues, etc, with the Ombudsmans office.	No	HHSA Full Support
CWS Resource Family Approval Portal	This new application replaces Child Welfare Services (CWS) adoptions application system currently hosted by CAIRS (CA6280) with a web portal hosted by Binti where resource parents can upload/submit completed forms and supporting documentation to become a foster care or adoption parent.	No	HHSA Coordinated Support
CWS Revolving Fund	Application to manage claims check for CWS program	Yes	HHSA SaaS Support
Cyberance	Cyberance DBA OnlineFileTaxes.com is in the Information Returns filing business since 2010. We have filed information returns includeing 1099, 1098, and W-2 forms for thousands of customers of all sizes. We have been offering Affordable Case Acts (ARA Reporting Services since 2015/ Within last year alone we filed close to half a million forms including 1095-B and 1095-C.	Yes	HHSA SaaS Support
DAS Bad Check Database	The Bad Check database keeps track of bad checks issued by customers. This database is a stand alone database and not linked with the Department of Animal Services main application Chameleon PA1136. Data for this app is entered from a debit memo from that is manually created when the bank returns a bad check.	No	PSG Coordinated Support
DAS Balance Due Report DB	The Balance Due Report database keeps track of payments due from customers. It is a stand-alone application and not linked to Department of Animal Services (DAS) main application Chameleon PA1136. Data is entered from a printed form from Chameleon.	No	PSG Coordinated Support
Data & Insights (formerly Socrata)	Socrata provides public data in the form of downloadable data sets, tables, charts, and graphs. This instance of Socrata will be an enterprise-wide service. Modules: Open Data Platform, Open Budget, Open Expenditures.	Yes	FG3 SaaS Support
Data Innovations Instrument Manager	Instrument Manager (IM) provides connectivity between laboratory instruments and County's Lab Information System STARLIMS, which aides in the flow of laboratory information, including test orders and results, specimen information and patient information. This solution will facilitate onboarding medical instruments, adding literally 1000's of device options. This will also enable to these medical devices to take advantage of the capabilities of the latest STARLIMS 12 platform which will be realized during the Upgrade and Rehost Project.	No	HHSA Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
DCSS ADHOC Shadow DBs	DCSS ADHOC Shadow DBs for all reporting and BI activities. DCSS business processes traverse three operational areas consisting of Administration, Legal and Operations. The Administration division of DCSS provides administrative support to the DCSS department. Administration contains six teams (Budget, Mail/File Bank, Human Resources, Payroll, Service Team and Tech). Administrative business processes that are impacted include: - Account Tracker access database (SQL backend) used to maintain a history of user accounts and their access levels - Asset tracking access database (SQL backend) used to maintain inventory of State owned IT devices - Internal Help Desk access database (SQL backend) used to internally control IT help tickets not associated with NGIT service - File Room ELFs (Electronic Filing System) application (Cold Fusion - SQL) used to maintain an assignment history and specified location of hard copied case files - Service Tracking Application (Cold Fusion - SQL) used as a historical and up to date service process history of legal serves to Non Custodial parents to appear in court. - SQL Reporting (Business Intelligence). Although this process is still under development, it will meet an important business need once established. Using information pulled from the State data warehouse and stored on an NGIT managed Virtual Server, Business Intelligence tools will be used to create ad-hoc reports The Legal division is comprised of Child Support Attorneys, Paralegals and Legal Clerks who provide legal representation to Superior Family Court dockets and walk in customers. Legal business processes impacted by this project include: - CAT Court Calendar application (Cold Fusion - SQL backend) which is used as a DCSS courtroom scheduling tool that provides court calendar scheduling. - Customer Dashboard application (Cold Fusion - SQL backend) which provides a	No	PSG Full Support
DCSS OKTA System	Multi factor remote logon solution for DCSS. It consists of two components that require installation: OKTA AD Agent. Note reports that need to be run off of OKTA cloud site: 1. Reports – MFA usage, 2. Reports – System Log Force of Activation EMAIL from OKTA – AD Settings TAB must be done as a toggle “ON or OFF”	No	PSG Coordinated Support
DCSS SFTP for Sheriff's Department	Secure file transfer between DCSS and Sheriff's Department.	No	PSG Full Support
DCSS State Dropbox	The system is used as drop box to transfer and receive DCSS related files via FileZilla sFTP client, which installed on the Standalone server.	No	PSG Coordinated Support
DCSS Wallboard System	Wallboard system for the San Diego Local Child Support Agency (LCSA) Call Center. RMG Enterprise Solutions that fluidly integrates with Genesys software. The new system will provide added customization features for business intelligence and program improvements to help call Center realize new efficiencies for the department and its customers and help LCSA achieve its strategic goals	No	PSG Full Support
Deaf Link	"Deaf Link is used to translate emergency public information into American Sign Language to recipients that have selected to receive their alerts in that format. Namely the Deaf, Blind, or hard of hearing. Deaf Link also performs ASL interpretation via teleconference in emergency shelters.	Yes	PSG SaaS Support
DeedAuction	Online service that helps facilitate the sale of tax defaulted properties via an online auction.	Yes	FG3 SaaS Support
DGS Generic Filing Cabinet	The DGS Generic File Cabinet was established to provide a central place to store an access documents. The business reason for choosing Documentum over Windows is so that, by policy, the paper copy of each document may be discarded once imported into the repository. In addition, the Personnel Folder provides a supplemental function for storing personnel records that fall outside the scope of responsibilities for the Department of Human Resources. In 2014, the DGS Generic File Cabinet was migrated to the new Enterprise Document Processing Platform (EDPP). This PAID has the following characteristics: • The DGS Generic File Cabinet resides in the COSDGEN Repository • There are no other applications associated with this PAID • Users import and access content directly through CARA • Folder Navigation and basic search tools are used to locate content • There are no custom jobs, workflows or coding • The Personnel Folder is the only folder with indexing	No	FG3 Coordinated Support
DHR BENEFITS ELECTRONIC DOCUMENTS UPLOAD	DHR BENEFITS ELECTRONIC DOCUMENTS UPLOAD system is a simple and easy to use web interface that will allow DHR users to import Benefits documents into the DHR Documentum repository. Features:• The Benefits Division of DHR will use this import tool to import electronic documents into DHR Documentum Repository. • System has the ability to convert different format (.doc, .xls, .jpeg, .png, .tiff & .bmp) documents to PDF• System has the ability to track the document / batch progress from Web Import tool until it reaches Documentum repository.• System has the ability to save the incomplete uploads and complete them at a later time.• System has the ability to auto-populate relevant data from PeopleSoft based on Employee ID.• System has the ability to import the Following Benefit Document types to the Documentum repository.o DHR COBRA Documentso DHR Benefits Misco DHR Beneficiary Designationso DHR Enrollment Formso DHR Personal Worksheeto DHR Confirmation Statemento DHR FMLA Misco DHR Temporary Employee.	No	FG3 Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
DHR BI Gateway	This is a Business Intelligence SaaS based system utilizing Microsoft Power BI services for the county of San Diego. Power BI services are used to publish and share reports, analytics, and dashboards in the cloud. Power BI service for Premium capacity provides a dedicated space with greater performance and scale. Additionally Power BI on-premise Gateway Services facilitates data synchronizations from the production data sources to the Power BI datasets.	No	FG3 Coordinated Support
DHR Captiva7 Scanning	DHR uses the Captiva product to handle their scanning, indexing, and conversion of documents that they release to Documentum for their document storage. The groups and the types of documents that they scan are: DHR Services: Employee Master Job and Non-Job docs, DHR Staff and DHR Exec documents Class Info docs, Car docs DHR Background Investigations: I9 docs DHR Benefits: Benefits docs	No	FG3 Full Support
DHR Document Repository for Medical Standards	DHR's Documentum and associated Captiva Capture system for scanning in medical standards documents and managing documents on-line using the DHR File Room Repository System. Wave-TSG developed the software and processes to capture the documents using Captiva tools and export the documents to Documentum.	No	FG3 Full Support
DHR Internet Class/Comp info.	Provides Class/Comp. Info on the internet	No	FG3 Full Support
DicksonOne DataLogger	Temperature monitoring hardware used in vaccine storage facilities, uploaded to cloud service, alerts set to specified users when temperature thresholds exceeded.	Yes	HHSA SaaS Support
DIMSNET	ROV Core Application..DIMS-Net Voter Registration Management System offers jurisdictions of all sizes a streamlined and integrated end-to-end voter registration solution as well as statewide voter registration systems to meet Help America Vote Act requirements. In Feb. 2020, Tenex ePollbooks were added, which uses the Panorama API to get data from DIMS. 9/7/21: For EAA users, the DIMNSET config file located on the user workstation, C:\program files\DIMS\DIMS.NET\DimSnet.cfg. should use the FQDN (Fully Qualified Doman Name) ussdscosd201.cosd.co.san-diego.ca.us.	No	FG3 Coordinated Support
DISC	DISCcert, LLC provides the County of San Diego the DISC Styles Assessment to aid the Department of Human Resources (DHR) in improving individual and team performance, nurturing and retaining top talent, developing leadership at every level of the organization and reducing workplace conflict.	Yes	FG3 SaaS Support
Disclosure Docs	Processes Form 700s Disclosure Documents in central repository.	Yes	FG3 SaaS Support
Diskriter, Inc.	Transcription of Psychiatric and medical dictation	Yes	HHSA SaaS Support
DMV Access	Enables approved County users to access CA DMV application	No	FG3 Full Support
Documents Capture for Loss Prevention Unit	This application expands the Documentum Repository System and associated ImageTrust Scanning System to accommodate Loss Prevention Unit documents which includes scan profiles incorporating appropriate features such as duplex scanning, back page dropout, auto rotate where supported, for 5 new batch classes (OSHA, Insurance Review, CEP, SEP, Historical)	No	FG3 Full Support
DocVault	Repository for all project/work request documentation	No	FG3 Full Support
DOJ Grievance Hearing	The DOJ Grievance Hearing Unit is used to collect information on the DOJ Grievance Hearings	No	HHSA Full Support
Don't Think Know (DTK)	This website allows young women, 25 years old and younger, in San Diego county to order free chlamydia and gonorrhea home test kits (in alignment with Centers for Disease Control and Prevention recommendations).	Yes	HHSA SaaS Support
DPW Referrals System	The Referrals database system tracks referrals from the CAO and the Board of Supervisors and provides management status reports.	No	LUEG Coordinated Support
EBIX	Certificate of Insurance Management Services - Tracking ToolCSAC-EIA awarded the contract	Yes	FG3 SaaS Support
ebtEDGE	The program is apart of the Statewide EBT System. It is a state support ASP.	No	HHSA Coordinated Support
eCivis Allocate	eCivis Allocate is a cloud-based, multi-tenant, SaaS solution that provides Cost Allocation services. The Cost Allocation Plan (CAP) is a formal means of accumulating and identifying indirect costs and central support service charges that ensures each department bears its fair share of the total costs for services. The application is hosted on the Google Cloud, which provides a secure stack from physical controls to data storage.	No	FG3 Coordinated Support
Eco-Visio	Visitor count data analyses are presented in the form dashboard. Data is visible at any given moment, saved in real time on the SaaS solution. Dashboards consist of a variety of interactive dynamic data visualization modules.	Yes	LUEG SaaS Support
Efforts To Outcome	ETO Software™ allows users to quantify and qualify the efforts that create and foster the client and inter/intra-agency relationships that drive the human services industry. ETO™ provides a structure and a common language for relationship management, analysis and decision-making at every level of an organization. It has been determined that ETO meets the requirement for CWS. In addition, other counties within California use ETO to meet the same requirements in a hosted (ASP) environment.	No	HHSA Full Support
Efforts to Outcomes (ETO) - PHS	Note: State hold this contract - see attached ETO software is a web-based, remotely hosted application being used by the State of California, Department of Public Health as the new data collection and reporting system for the Black Infant Health (BIH) Program.	Yes	HHSA SaaS Support
eForms Repository	This is to store eForms during and after their business lifecycle with the idea that this App may be shared by multiple county departments and agencies that don't have their own storage solution.	No	FG3 Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
EK Health - Managed Care	Its a SaaS system that does not have a direct cost to it. The way the cost component is structured is the vendor while providing three distinct services to the County will be paid just a flat fee per transaction for the two of three services and a flat fee plus percentage for the third service. The system itself wont cost anything, there is no maintenance or licensing fee or any IT related charges.	Yes	FG3 SaaS Support
Electronic Approval Workflow	This application is to automate the countywide routing and approvals of Board Letters and related documents to improve efficiency and reduce costs. Workflow automation supports the County's Green Initiative by reducing automobile traffic associated with manually processing Board Letter documentation, in addition to aligning with the County's Required Disciplines of Information Technology, Continuous Improvement and Fiscal Stability. Key Functionalities Ability to obtain secure, documented electronic approval/rejection of documents from any County computer, off-site computer or any smart phones allows IMAPI 24 hours a day/7 days a week without manually transporting materials. Full functionality must be available from network desktop computers and off-site computers (with use of VPN). Approval functionality must be available from any smart Phone allows IMAPI.	No	FG3 Full Support
Electronic Municipal Market Acces	The Electronic Municipal Market Access website, or EMMA®, is the official repository for information on virtually all municipal securities. EMMA provides free public access to official disclosures, trade data, credit ratings and other resources and tools for understanding the municipal securities market. EMMA is an award-winning website, recognized by the National Federation of Municipal Analysts and the National Association of State Treasurers' State Debt Management Network. The Municipal Securities Rulemaking Board (MSRB) operates the EMMA website under authority granted by the U.S. Securities and Exchange Commission (SEC).The EMMA website was established to increase the transparency of the municipal securities market by providing free public access to municipal securities disclosures and data. EMMA provides investors, state and local governments and other market participants with key information and tools to put that information into context.	Yes	FG3 SaaS Support
Electronic Public Document Library	Website for allowing public to search and retrieve APCD documents. San Diego County Air Pollution Control District is required by Assembly Bill 423 to make documents available to the public through a public search Website, effective by the end of calendar year 2021. APCD will define the record types and associated document types to be made available to the public through the public search website, available on the internet.	No	Other Full Support
Eligibility Case Comments	CalWIN, Welfare-to-Work (WTW), and QESD Case Comments tools allow the user to collect information from a customer. All the information captured through the use of several sub-forms is consolidated and displayed at the bottom of the main form so the user can copy and paste it into a different system. These tools do not have a back-end; Information entered is not saved. HTML, JavaScript, and CSS were used to create the user interface (main form and several sub-forms).	No	HHSA Full Support
Elite	The Application contains data used to determined initial and ongoing eligibility for rental assistance for qualified residents of San Diego County. It also generates rental assistance payment to landlords. Data included the database is personal information and financial record. Data is to be treated as highly confidential.	No	HHSA Full Support
Emergency Aid Tracking	This application is used to track information related to children receiving emergency aid, and related family members. The application tracks this by creating a case number, and then associating impacted family members to the case, along with a questionnaire. The application was previously part of a web app that was retired (PA2341), then migrated to Microsoft SharePoint, and now is on the Microsoft Dynamics CRM 2016 Framework.	No	HHSA Full Support
Emergency Rental Assistance Program	This application assists with the provisioning of housing funds for Covid19 victims. It is also known as ERAP for short. The application was created and will be supported by Basc LLC and hosted on AWS.	No	HHSA Coordinated Support
Emissions Inventory System	The Emission Inventory System (EIS) application replaces the old desktop EASIER system with a modern, stable, web-based application that addresses the technological limitations of the existing legacy application by supporting internal staff in addition to the target regulated community and other external parties. The new EIS more effectively supports and facilitates the core functions of APCD's Toxic Emissions Inventory Section (within the Engineering Division) and provides extensive and flexible ad-hoc and standardized reporting capabilities, caseload management tools, workflow management, and a modern, intuitive user interface. EIS fits County of San Diego's Land Use & Environment Group's vision "to create a collaborative environment that empowers the Citizens and County Staff, and enables the LUEG business processes to deliver high value quality services in the most efficient and timely manner."	No	Other Full Support
emocha Mobile Health Inc.	emocha adherence solutions provide tools to improve patient adherence to medication and treatment. Through video-based Directly Observed Therapy (VDOT), patients can report symptoms and record themselves taking medication at their own convenience, while providers assess videos and adherence analytics on a web-based portal. emocha is used around the world to monitor adherence through VDOT, smart-pill bottle integrations, SMS reminders, and more. The platform has been a solution for opioid addiction therapy, hepatitis C, and tuberculosis medication adherence.	Yes	HHSA SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
EMS LEMSIS Data Mart	The EMS team is currently migrating to a cloud system from ImageTrend which does not have the flexibility in reporting needed for Epidemiology trending. Therefore, the data gathered in the ImageTrend system will need to be sent to the County and put into a DB for complex querying on a daily basis. EMS also needs a replacement tool for MS Access to pull data from the SQL DB into SPSS.	No	PSG Full Support
Energy Management	BuildingOS is a comprehensive cloud based software solution that manages building performance and energy consumption across County facilities. The system shall includes an ability for necessary customizations to allow the County to deliver actionable building intelligence. The system integrates with the existing Builiding Automation Systems and the Tririga application.	No	FG3 Coordinated Support
Enterprise Document Processing Platform	This platform will be used to host all Documentum applications.	No	FG3 Full Support
Enterprise Email Solution	The Enterprise Email solution consists of two parts. 1. A website that email submissions are posted to from multiple County websites. The email is either processed and sent to IronPort for delivery or a record in written to the WEBPROD email database.2. An executable runs every 1 minute and reads the email database table on the WEBPROD database. All records with a status of zero (unprocessed) are read and processed and sent to IronPort for delivery. Successful entries are then deleted from the table. Entries that have errors are flagged for later review.	No	FG3 Full Support
Enterprise Oracle BI	The intent of the DW is to create metadata that can easily be accessed and manipulated for report generation and analysis, move the County to new technology, allow users to join data from various applications (i.e., Oracle E-business, Kronos Timekeeping, PeopleSoft HR and Payroll, Performance Budgeting, Documentum, Itrack) for reporting, and provide end users with an overall robust and flexible data analytical and reporting capability	No	FG3 Full Support
EOS	Library/publication tracking	Yes	FG3 SaaS Support
EPI HIE SFTP Access	This application is a user interface from 4 CoSD workstations to the Health Information Exchange (HIE). The HIE allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically, improving the speed, quality, safety and cost of patient care.	No	HHSA Full Support
ePoll Book - ROV	ePoll books allows an ROV election worker to check-in a potential voter, identify ballot type, and print a confirmation receipt. Each ePoll book aka touchpad has a copy of all 1.8 million registered voters in San Diego County. This system vendor is TENEX was procured via DPC RFP 9595. The solution is certified by the CA SOS.The ePoll book will securely connect via WiFi via Cradlepoint device running dual SIM cards (AT&T and Verizon). Perspecta will be providing and managing the Cradlepoint for each election. Precinct Central (TENEX cloud solution) has a highly fine-tuned, performance-tested strategy for data updates. The robust communication framework ensures all locations are current with voter information and guards against double voting. The basic process flow for real-time updates behaves as follows: Each Touchpad is connected to a secure Cloud repository through a secure Cradlepoint connection. Using the secure connection, changes made at the elections office are automatically communicated to all Touchpad devices at all voting locations. At voting locations, as voters check in on the Touchpad, their vote type, ballot style, time, location, and operator are all saved to their voter record. This information is securely transmitted to the central server. All information received at the central server is packaged and securely pushed out to all Touchpad units at the voting locations. If a voter attempts to go to another voting location to vote, the poll worker will see that the voter has already voted and what method the voter voted by. While Precinct Central is fully capable of communicating information across the jurisdiction in real-time, it is important to note, that the connectivity and real-time updates are not a requirement to operate the electronic poll book. In the event that connectivity is lost or not available, each Touchpad is fully capable of operating stand-alone. Further, each Touchpad directly communicates to other Touchpads at the vot	Yes	FG3 SaaS Support
ERMS Bin Tracking	Bin Content Tracking is a web-based application utilizing Barcodes and readers for entering and tracking the status & location of documents being processed at the DPC.	No	HHSA Full Support
ERMS CCS	This application is for California Children Services Program will use for Client document management.	No	HHSA Full Support
ERMS CWS	CWS ERMS and CWS Document Processing Center (DPC). Viewer and DPC facility going live together to support the Child Welfare Services operations. 6 Regions to be deployed as part of solution.	No	HHSA Full Support
ERMS Forms Library	Document Type inventories and Category/SubCategory organization, and also holds the official, barcoded sample form files used with those repositories	No	HHSA Full Support
ERMS HCDS	Housing Community Development Services (HCDS) ERMS	No	HHSA Full Support
ERMS HSHB	The HSHB ERMS Application was created to provide a user-friendly means for importing, searching and retrieving these documents.	No	HHSA Full Support
ERMS PAPG	Public Administrator/Public Guardian (PA/PG) ERMS	No	HHSA Full Support
ERMS PC	Public Conservator (PC) ERMS is an application that PC uses for Electronic Document Management	No	HHSA Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
ERMS QDocs PI-QESD	The PI/QESD department of HHSA performs audits of the CalWIN program. During the process of a typical audit, documents supporting CalWIN cases to be audited are copied from the CERMS electronic document system and physically placed in a folder. These documents are arranged in a manner dictated by state and federal requirements, and identifying audit Element Numbers (also provided by state and federal agencies) are handwritten on each document's facing page to maintain its order in the file. When the paper audit file is complete and ready for submittal, it is scanned to generate a single PDF file and emailed to the various agencies.	No	HHSA Full Support
ERMXtender for ARCC	ERMxtender to convert reports from the Mainframe to online images.	No	FG3 Coordinated Support
ERP Oracle Financials	Comprises : GL(general Ledger) AP(Accounts Payables) AR(Accounts Receivables) CM(Cash Management) FA(Fixed Asset) HR modules Purchase Order P.O.:standard,blanket,planned,contract) Requisition RFQ(Request for Quotation) Quotation Grants Accounting Projects	No	FG3 Full Support
ERP Website content management	The ERP Information Center solution enables CoSD staff to maintain forms, reports, and information in various file formats (Word, PDF, etc.) CoSD staff upload files to SharePoint document libraries; from there, files become available to users on the ERP Information Center intranet website.	No	FG3 Full Support
eSIMs	Electronic Laboratory Notebook.	Yes	Other SaaS Support
Ethics Hotline and Website	Provides a means for the public to confidentially report fraud, abuse and other complaints	Yes	FG3 SaaS Support
eTime	DEH Time Entry Form application - It is a form that allows DEH users to record their time against Accela inspections and administrative tasks. The form simplifies the process inspectors use today to enter their time sheets	No	LUEG Coordinated Support
E-Track	This is a web based CRM application. The E-Track (formerly named PA Enrollment) application will support the HHSA Public Authority group to maintain a list of individual providers who provide service for consumers receiving In-Home Supportive Services (IHSS). Providers enable low income seniors and disabled Consumers to live independently in the comfort of their own homes.	No	HHSA Full Support
Eventbrite	Free service that allows public and County employees to register for the annual economic roundtable forum.	Yes	FG3 SaaS Support
External Agencies WEB Reporting	Allows External and Internal Agencies to generate or view daily, monthly, quarterly and yearly specific reports for their agency only. There is a directory drill down capability for predefined generated reports. Each External Agency must log onto the SPOL with given userid and password.	No	FG3 Full Support
EZ Access	Unsecured Property Assessment For Business inventories, Marine vessels, Aircraft, Leasing & Leased land, Agriculture	No	FG3 Coordinated Support
EZ Access - Jwalk	GUI emulator	No	FG3 Coordinated Support
EZ Access Interfacing Systems	Vendor application that resides on the AS/400 and provides CoSD unsecured property information.	No	FG3 Full Support
EZ Book	Used to book reservations for conference rooms in COC and CAC Application was procured by COB, transferred to DGS with management of CAC This app was approved when it was owned by FGG/COB It is currently in use at COC and CAC. Renewal dates are different	Yes	FG3 SaaS Support
EZTrak	Manage inventory for Public Health Warehouse in real time.	Yes	HHSA SaaS Support
Facebook	Social Media Site	Yes	FG3 SaaS Support
Facil	Facil Data Management Software for Media Access CentersFacil is a comprehensive data management system for organizations providing Public, Educational, or Government media access. These organizations operate video production facilities, lend equipment, train and assist their users in production, program channels for cablecast or other distribution, perform community outreach, and more. The Facil system includes contact management, equipment inventory, complex equipment and facilities scheduling, class scheduling and registration, channel scheduling, volunteer management, project and program tracking, point of sale, mailing list and mass email functionality, and more. http://www.beckersoftware.com/facil/index.htm	No	FG3 Coordinated Support
Farmers Market	Farmers Market app was built by CityGovApp. The app is used to conduct inspections of commercial agricultural growers selling products at certified farmers markets, and the market operation.	No	LUEG Coordinated Support
Federated Records Management	Federated Records Manager (FRM) facilitates control of the entire corporate record lifecycle creation, safeguard, access, and destruction according to a broad range of system-enforced policies. This electronic records management tool helps the CoSD comply with the recordkeeping requirements of regulations and leverage uniform policies across all formats and depositories.	No	FG3 Full Support
Field Survey Notes Index	Database to maintain and research field survey notes	No	LUEG Full Support
FirstWatch	This is an business intelligence application owned by CAL FIRE that receives information from the CAL FIRE dispatch system.	Yes	PSG SaaS Support
Fleet Focus M5	DGS uses M4 product for vehicle asset management, maintenance management, and fuel managementM4/M5 is the only product that includes ALL functionality required for fleet management without the need to integrate with a third party product for fuel	Yes	FG3 SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Fleet Management Information System (M5)	The Department of General Services, Fleet Management Division (Fleet) is responsible for managing the County's fleet of vehicles. M5 is the system of record for all activity related to County vehicles. M5 is used to track vehicle acquisition/disposal, vehicle maintenance, vehicle fuel consumption, and part inventory. Since 2001, Fleet's M5 environment has been hosted by AssetWorks at its data center in Wayne, PA and is accessed via the internet using an encrypted connection. AssetWorks SaaS/ASP not only includes hosting the application, but also includes break/fix resolution, database administration, backups, disaster recovery, training, application patches, and version control. The application is assigned PAID1268.	No	FG3 Coordinated Support
Gale in Context - Homework Suite	Gale in context Homework suite for Elementary, Middle School, and High School provides age appropriate reference content, biographies, primary sources, multimedia, critical essays, news, charts and graphs, videos, academic journals and more. It helps students gain comfort with research by delivering age appropriate, reliable, curriculum-related content covering a broad range of subjects taught in the classroom like animals, arts and music, social studies, health, history, government, language arts, and more. It also offers resources for creating papers, projects, and presentations. This database is aimed at older elementary, and middle and high school aged students.	Yes	LUEG SaaS Support
Gale Presents - Udemy	Gale Presents: Udemy connects patrons to more than 8,000 video-based online learning courses in business, technology, and personal development. Udemy is a database of video-based courses geared to adults to help them advance in their careers, learn new skills, or practice new hobbies. The courses may include instructor lectures, slides, screencasts, articles, or quizzes. Courses typically include a hands-on component that is practical and allows learners to apply their new skills; approximately 60 percent of courses include supplemental materials such as assignments, quizzes, practice tests and coding exercises. These materials include PDFs, design templates, sheet music, source code or links to external websites.	Yes	LUEG SaaS Support
GASB87 Compliant Lease Accounting	Lease accounting system that calculates the County's real property and personal property leases.	No	FG3 Full Support
GNET Cloud	NEW Cloud Version of Exiting DAD GraniteNet used to conduct CCTV inspections of Wastewater / Sewer Networks, and to provide reporting capabilities.	Yes	LUEG SaaS Support
Google Enterprise Search	Enterprise search functionality for websites	Yes	FG3 SaaS Support
Google Forms & Google Sheets	A registration and assessment survey has been developed using Google Forms. The information entered into this survey is linked to a customized Google Sheet workbook that contains a dashboard, program highlights and action plan tabs. Links to helpful resources are embedded within the workbook to help organizations improve overall workplace health wellness. Data collected is considered LOW RISK.	Yes	HHSA SaaS Support
GovDelivery: Email Subscription	ASP Email Subscription service to notify the public when changes have been made to pages they have selected. Email Services	No	FG3 Coordinated Support
Grammarly Business	Grammarly Business is an AI powered writing assistant that checking spelling, grammar, tone and clarity of communication. It provides in-text feedback. Grammarly encrypts all data in transit and at rest. Data transfer is protected using the industry-standard TLS 1.2 protocol, while data at rest in AWS is encrypted using AES-256 server-side encryption. Grammarly uses AWS Key Management Services for database encryption and secure key management.	Yes	FG3 SaaS Support
Granicus Peak Agenda Management	This application is used as an agenda management system. It allows for automating agenda creation, approval, management and publishing processes as required per Assembly Bill 423.	No	Other Coordinated Support
Hadronex SmartCover	The Hadronex system is a satelite linked set of mointoring devices which measure the level of sewage for certain manhole covers. County Wastewater staff are alerted of potential spills. There is a vendor hosted website which can be used to monitor the status of all Hadronex locations.	Yes	LUEG SaaS Support
HandsOn Connect	Volunteer management system that will be able to offer volunteer tracking, scheduling and recruitment services.	Yes	LUEG SaaS Support
Hanna Interpreting Services	Hanna Interpreting Services oral translations services by professional language interpreters to County departments where a need for interpretation services has been identified.	Yes	FG3 SaaS Support
Hanna, Video Remote Interpretation	AWS is the largest provider of cloud services globally supporting over 1 million active customers in 190 countries. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards, including: SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), SOC 2, SOC 3, FISMA, DIACAP, and FedRAMP, PCI DSS Level 1 Ø ISO 27001, ITAR, FIPS 140-2	Yes	FG3 SaaS Support
Health Outcomes Management System (HOMS)	Manages the HOMS web based DB used by Behaviorial Health provides to track client outcomes.	Yes	HHSA SaaS Support
Help Me kNow Hub	Virtual and on-demand training for Microsoft applications. Training videos, virtual classes, 1:1 training/support via phone/chat. Available at helpmeknow.sandiegocounty.gov and HelpMeNow app in Teams.	No	HHSA Coordinated Support
HHSA AIS Case Management Kofax Imaging	Provide a content management solution for AIS Case Management System with Kofax & HHSA Imaging. This application provides management system to provide case digital content.	No	HHSA Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
HHSA Application Xtender	Application Xtender is a content management solution that scans, stores, retrieves, and preserves information, while providing role-based access from nearly any device or web browser. This application tool is being used to lookup scanned Death Records images and metadata for research. The HHSA environment uses two components of the tool (Web Extender and Document Manager).	No	HHSA Full Support
HHSA Privacy Incident Reporting DB	Privacy Incident Reports (PIRs) to be submitted by County Staff/Contractors to the HHSA Compliance Office via the internet. This application will allow Staff/Contractor to upload and manage (i.e., view and delete) files/documents related to the PIR being submitted.	No	HHSA Full Support
HHSA Program Guides	The County of San Diego, Health and Human Services use Documentum Web top to modify/add and publish their program guides to the county web-site. The County of San Diego use a Documentum-based solution for authoring CoSD Health and Human Services Agency (HHSA) program guide (the CalWORKs program guide) and publishing that program guide to a web site. The web site provides access to the documents that make up the program guide through a Table of Contents metaphor. The website also includes a search feature which provides search results scoped by program guide.	No	HHSA Full Support
Homeowner Exemptions - AS/400	Secured property generate homeowner claims for lien year processing of homeowner exemptions	No	FG3 Full Support
Hootsuite	HootSuite is a social media management tool that allows users to schedule and post updates to any page or profile for Facebook, Twitter, LinkedIn, Instagram, and other platforms from one placethe HootSuite dashboard.	Yes	LUEG SaaS Support
HR Documentum	Documentum web based application which allows the scanning, indexing, and retrieval of documents. It uses Kofax 10 for scanning, recognition, and validation of documents. Document are imported into the Documentum system and placed in the appropriate folders with the appropriate security. Webtop is using to retrieve the documents.	No	HHSA Full Support
HR Employment Document Management System	Documentum-based document management system to support collection, processing and reviewing HR employee and job application documents. Scanning of employment and employee-related documents, storage of all HR employee and benefits documents, and retreival of those documents via a Documentum web-based interface.	No	FG3 Full Support
HUD IDIS	As a nationwide database, the Integrated Disbursement and Information System (IDIS) provides HUD with current information regarding the program activities underway across the Nation, including funding data. HUD uses this information to report to Congress and to monitor grantees. IDIS is the draw down and reporting system for the five CPD formula grant programs: Community Development Block Grant (CDBG), HOME Investment Partnerships (HOME), Housing Trust Fund (HTF), Emergency Solutions Grants (ESG), and Housing Opportunities for Persons With AIDS (HOPWA); and for the CPD competitive grant program HOPWA Competitive. Grantees also use IDIS for Consolidated Planning.	Yes	HHSA SaaS Support
HUD Web Access Security Subsystem (WASS)	Housing and Urban Development Web Access Security System (HUD WASS). The purpose of WASS is to provide secure access to the HUD systems environment by their trusted business partners and internal HUD users. Currently, WASS provides access to over 15 systems for external users and over 20 systems for internal users.	Yes	HHSA SaaS Support
ImageTrend	ImageTrend is a cloud-based solution that replaces the QANet/QCS prehospital admissions system.	Yes	PSG SaaS Support
inLighten	The solution will customize and automate the County Treasurer/Taxpayers payment area with video monitors delivering targeted messaging, community images, useful information, news, weather, trivia, sports, stock information to provide taxpayers with an interesting source of information while standing in line.	Yes	FG3 SaaS Support
Innovative Millennium	The Millennium application is used to manage the business processes of San Diego County Library. The library Web site is included within this system. It is a COTS Unix-based system. The Library web-site is included within this system, along with bar-code scanning check-out capabilities. The Millennium system houses the data from the library. The Millennium server authorizes some 3rd Party website access from library and library patrons accessing the library from outside the Library. The Millennium application is available to the library system seven days a week from 0700 to 2000 hours Pacific Monday through Saturday and 1200 to 2000 Pacific on Sunday. The library is available with outside access via the web on a 24 hour basis. The Millennium system is currently in use by the County of San Diego Library.	No	LUEG Coordinated Support
iNovah Cashiering	The iNovah application is used to collect money directly from debtors. It is built around a consolidated payment database that serves as the central repository for all types of collections. iNovah is an Enterprise Revenue Management (ERM) solution for government cashiering that supports configurability, payment processing, security, PA-DSS PCI compliance, banking models, auditing, reporting, reconciliation, and real-time interface capabilities.	No	FG3 Coordinated Support
Instagram	Social Media Photo Site	Yes	FG3 SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Integrated Recording and Vital Records System (aka. ACCLAIM)	This Integrated Recording and Vital Records System which has been developed by Harris Recording Solutions. The system will support the following high-level functions: Recording, Scanning/Archiving, Vital Records, Indexing/Verification, Marriage License Application/Recording, System Administration/Controls, Fictitious Business Name Filing, Customer Search Services (Kiosks), Integrated Cashiering, Customer Search, Services, eCommerce (Web), Fully Integrated Accounting, Reporting, Transfer Tax Collection/Distribution, Interface with External Data Sources, Auto Indexing, Interface with CoSD Oracle Financials, eRecording/SECURE, Interface with CoSD Property Tax System, Integrated Redaction. Java not needed by the Application.	No	FG3 Coordinated Support
Interest Apportionment	Computes interest and Tax base on Cash balances	No	FG3 Full Support
Interpreters Unlimited eSAF Form and e-Workflow	Interpreters Unlimited (IU) delivers American Sign Language (ASL) translations services by professionallanguage interpreters to County departments where a need for interpretation services hasbeen identified.	Yes	FG3 SaaS Support
Intterra	Intterra is used by the County's Fire Authority to manage fire incidents, providing a picture of the incident on a moment by moment basis. It is an extremely valuable tool utilizing aggregated GIS data from a variety of sources - providing details of a specific incident, aiding the development of pre-plans, managing overall Fire operations and providing useful reporting and analytics.	Yes	PSG SaaS Support
ISCP - CODE 1 Plus	Vendor supplied Zip Code inquiry and correction software.	No	FG3 Full Support
ISSUE TRACKER SYSTEM	Solution for election call center/issue tracker system. This solution will be used by the Registrar of Voters staff to improve services provided to poll workers.	Yes	FG3 SaaS Support
IT Portfolio Management (MEGA)	MEGA's HOPEX platform offers a comprehensive, well-rounded, feature-rich platform that provides an out-of-the-box metamodel that is highly configurable and has strong modeling capabilities. It also supports a wide range of industry frameworks. HOPEX combines industry-leading practices in enterprise architecture (EA), IT portfolio management (ITPM), business process analysis (BPA), and governance, risk, and compliance (GRC) into a single platform. This integrated solution gives an interactive view of all business and IT components to help drive business and IT transformation	No	FG3 Coordinated Support
iTr App	iTrApp is an app built by CityGovApp to track glassy winged sharpshooter traps at commercial nurseries. Glassy winged sharpshooter is an insect that can transmit a disease called Pierce's Disease, this disease is deadly to grapevines in California	No	LUEG Coordinated Support
ITrack	Nicus M-PWR is an enterprise-wide IT financial management application used for IT chargeback, cost visibility, budgeting, and forecasting. It replaces the legacy COSD Chargeback system.	No	FG3 Full Support
iVOS	Workers' Compensation Claims. iVOS is a claims administration vendor product used by DHR. The application consists of a web front-end and a back-end database	No	FG3 Coordinated Support
JCATS-SaaS-Interfaces	The JCATS system has moved to the Canyon Solutions Cloud. This PAID covers all the interfaces between the JCATS-SaaS system and the County environment. The old JCATS on-premise environment will be retired (PA2103).	No	PSG Coordinated Support
Judicial Court Activity Tracking System (JCATS)	MOVED TO CANYON SOULTIONS (vendor). The Judicial Court Activity Tracking System (JCATS), is a Public Defender adult criminal, juvenile, and mental health case management system.	No	PSG Coordinated Support
Justice Electronic Library System (JELS)	SharePoint based Document Distribution, Managment and Attorney Tools to support paperless justice ecosystem. Note: Patching to this app requires that the database be taken out of high availability mode.	No	FG3 Full Support
Kahoot	Kahoot allows users to create, share and play learning games in an interactive session. This is a free tool in which participants do not need to create an account to participate.	Yes	LUEG SaaS Support
KnowBe4 Portal	KnowBe4 Portal is the vendor utilized for End User Security Awareness Training.	No	FG3 Coordinated Support
Knowledge Rocket	Chameleon is the core animal management system used by DAS. It is hosted on premise. One module, Knowledge Rocket, will pull extracts of animal records and transmit them to 3rd party hosts. One data set is the animals available for adoption and found animals. This data is added to a nationwide database of adoptable and found animals and displayed on the PetHarbor website. The other set of records is dog licensing information. This set of records is transmitted to the application vendor. The vendor manages on line licensing and credit card payment acceptance and clearing. Data about licensing fees paid is returned to the department and the payments received are cleared to the County bank account by the vendor. Vendor takes credit card data on their site from customer. Credit card data is transmitted back to County by the clearing bank so it is available in case of refund (lock box with Wells Fargo).	No	PSG Coordinated Support
Knowledge Rocket module of Chameleon	Chameleon is the core animal management system used by DAS. It is hosted on premise. One module, Knowledge Rocket, will pull extracts of animal records and transmit them to 3rd party hosts. One data set is the animals available for adoption and found animals. This data is added to a nationwide database of adoptable and found animals and displayed on the PetHarbor website. The other set of records is dog liscensing information. This set of records is transmitted to the application vendor. The vendor manages on line licensing and credit card payment acceptance and clearing. Data about licensing fees paid is returned to the department and the payments received are cleared to the County bank account by the vendor. Vendor takes credit card data on their site from customer. Credit card data is transmitted back to County by the clearing bank so it is available in case of refund (lock box with Wells Fargo)	Yes	PSG SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Knox Connect	Knox Connect manages access and maintains a log of master key access for emergency personnel.	Yes	PSG SaaS Support
Kronos HHSA Workforce Analytics	Enables analysis of scheduling to optimize workforce deployment. San Diego County Psychiatric Hospital - 45281.	No	HHSA Full Support
Kronos Workforce Central	Time Collection System	No	FG3 Full Support
LAFCO ApplicationXtender (AX) Imaging Environment	LAFCO is currently leveraging ARCC's Kofax document scanning and ApplicationXtender (AX) environments for their document content management requirements. They are about to embark on an extensive "back-file" scanning effort for their historical documents/records, and implementing new day-forward scanning procedures. This project includes the implementation of new infrastructure to support their full-text search requirements and configuration of separate Centera Immutable Storage Pools that is consistent with the AX File Access Manager (FAM) environment	No	FG3 Full Support
LCPtracker Professional	LCPtracker Pro is a cloud-based prevailing wage and workforce compliance management solution. The application is ideal for public agencies and prime contractors that need to ensure all contractors on their project, even down to the lower-tier subcontractors, are compliant. Additionally, clients can track detailed worker information and leverage dynamic reporting to monitor workforce initiatives.---------- accounts/access are handled by Vendor	No	HHSA Coordinated Support
LeagueLineup	League Management Software	Yes	LUEG SaaS Support
Learning Health Care Network (LHCN)	With UC Davis oversight, there will be a development of an EP LHCN software application (app) to support the ongoing data-driven learning and program development across the state. This LHCN will collect and visualize real-time data at the individual, clinic, county and state levels to inform consumer and program level decisions and develop learning opportunities for individuals, staff, programs and administrators, in order to improve consumer outcomes. In addition, this project will include training and technical assistance to San Diego identified EP providers to help them fully utilize the data in routine clinical care. The associated evaluation will examine the impact of the LHCN on the EP programs, and will quantify the cost of implementation and utilization, in order to support statewide efforts for early identification and treatment of psychosis. This project is an innovative approach to state-level learning and real-time outcomes monitoring for consumers, their families, and the identified EP Provider in San Diego. Additionally, this project allows for collaboration and learning between other designated participating Counties in California with EP programs.	Yes	HHSA SaaS Support
Lectora Online	Online training development tool	Yes	FG3 SaaS Support
Lexipol On-line Policy Manual Development Service	Lexipol is used to manage the departmental policies for Probation.	Yes	PSG SaaS Support
Lexis State Net	Legislative Research Tool hosted by LexisNexis. LexisNexis State Net is the premier online legislative and regulatory intelligence and tracking application forthe 50 States and Congress. State Net allows clients to monitor and manage pending legislative and regulatory activity so they can confidently assess the impact to their organization. County users enter commentary and notes into system and use workflow to manage legislative analysis process.	Yes	HHSA SaaS Support
Liquid Web	Hosting and support of County News Center on the current Rackspace cloud server www.countynewscenter.com	Yes	FG3 SaaS Support
LiveChat Software	Chat software (plug-in) to initiate chat service between customers via their Internet web site and child support managers (CSM)	No	PSG Coordinated Support
Livestream	Live streaming service used along with a Livestream encoder for CCO broadcast events.	Yes	FG3 SaaS Support
LiveWellSD.org (AEM)	LiveWellSD.org website hosted on AEM platform. This site does not share the main County AEM website templates.	No	HHSA Full Support
Lobby Central	Public customer check in system.	Yes	PSG SaaS Support
LUEG Data Warehouse	Operational Data Store (ODS) for the LUEG team to query against using Power BI. There are several ETL jobs that move the production data from Accela Production Database to the LUEG ODS on a daily basis during off business hours.	No	LUEG Full Support
LUEG Documentum Import Tool	The application is generally used by the Land Use and Environment Group for uploading the documents from a CD/file location to Documentum. The users log on to the application by typing in their County credentials (User name and Password) for SSO verification and determination if she or he is a valid user of the tool. Once the credentials are authenticated, the user selects from which folder the documents will be into Documentum. After the selection, the user then locates the CSV file which has the document information (i.e.: object name, documentum folder, permit type, permit number, and subtype). Once the the CSV is dragged onto the application import region, the application will begin its validation process. If the validation process is successful, the application will automatically begin the import process.	No	LUEG Full Support
LUEG Repository	The departments of Air Pollution Control District, Agriculture Weights and Measures, Environmental Health, Planning and Development Services and Public Works, have implemented an electronic document management solution to automate the business processes for creating, storing, retrieving, routing, and distributing documents associated with parcels, permits, inspections, and other business processes.	No	LUEG Full Support
MailChimp	Mailchimp is a marketing automation platform and an email marketing service.	Yes	HHSA SaaS Support
Manual Clearing Database	Admin Utility, Engineering Services	No	FG3 Coordinated Support
Marshall-Swift Commercial/Agricultural Estimator	3rd party vendor application used to appraise commercial real estate	No	FG3 Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Master Background Investigation Database	Department of Human Resources Background Investigations database used to track progress of investigations conducted on employees and contractors for the county of San Diego.	No	FG3 Coordinated Support
MBTI by CPP	"CPP, Inc. is the Employee Development Divisions (EDD) vendor to provide the Myers-Briggs Type Indicator (MBTI) instrument. Training participants go into the system and answer a series of questions in order to have their personality type determined. EDD provides trainings in each of its Academies to interpret the results so training participants understand themselves a little better in order to work with others more effectively	Yes	FG3 SaaS Support
Medical Standards In-service Tracking	Personnel immunizations and health screenings tracking system.	No	FG3 Coordinated Support
Medical Therapy Unit Online	State Developed software hosted locally for CCS for tracking and generating reports to the State.	No	HHSA Full Support
Mendoza Daily Diary	This system is the construction inspection system for capital improvement projects.	Yes	LUEG SaaS Support
Mental Health Conservator/Case Management	The Health & Human Services Agency (the Agency) uses Panoramic Software Inc.s Windows-based application to record, monitor, and manage fiduciary funds on behalf of clients. The system is also used for case management services and programs rely exclusively on Panosoft for form creation and retention, electronic health record, and database needs.	Yes	HHSA SaaS Support
MHSA Data Collection & Reporting System	Reporting System is a State system that collects client level service utilization data about California's county mental health programs. Data are provided monthly by county mental health programs (MHPs) and summarized at the state level. It is a requirement and is used to provide service utilization data to DHCS management and staff, MHPs, other state agencies, federal agencies, the Legislature, and other interested groups and individuals	Yes	HHSA SaaS Support
Minerva	DPW Recycling Landfill Diversion Management; SaaS based application support by the vendor MSW Consultants	No	LUEG Coordinated Support
Mission Manager	Mission Manager is a Cloud based application that is used to coordinate and manage volunteer efforts in emergency situations. It has been used by DAS in the past as a No Charge service. The vendor now wants to charge for it. It is currently in use by the Sheriff s Department. Application contains basic information about the volunteer including name, address, phone, and e-mail. It also allows the volunteer to enter medical information (such as allergic to bee stings), hence the confidential classification	Yes	PSG SaaS Support
MPI Card Viewing Application	BHS/HIMS (Health Information Management Services) Scanning application and repository for an estimated 250,000 MPI (paper Master Patient Index) cards that needs to be stored/archived permanently. HIMS has an estimated 250,000 MPI (Master Patient Index) cards that needs to be stored/archived permanently. Each MPI Index Card holds Patient Name, Date of Birth, Medical Record Number, Social Security Number, S# and Encounter Dates.	No	HHSA Full Support
MPR Online	Online inquiry	No	FG3 Full Support
Multiple Senior Services Program	Multiple Senior Services Program - case management, purchase services, & case tracking	No	HHSA Coordinated Support
Mural	Collaboration platform used to guide and engage participants.	Yes	LUEG SaaS Support
myCAvax (CalVax)	CalVax will provide CRM (Customer Relationship Management) Tracking for vaccine patients, supply management for vaccines, contact management including alerts and notifications via SMS text or email as well as analytics and reporting for COVID-19 vaccines and potentially other vaccines as well.	Yes	HHSA SaaS Support
myRequests	Production Web Server for myRequests	No	FG3 Full Support
Nationwide	Deferred Compensation participants' account for plans they are enrolled in. Can administer their accounts online. Nationwide is exempted from public records pursuant to CA Govt Code § 6254(c)	Yes	FG3 SaaS Support
NeoGov	County Application's Management system. The web site https://login.neogov.com/ hosted by the vendor.	No	FG3 Coordinated Support
Nice InContact	Vendor-hosted and supported call center software used by three HHSA Program call centers: SSS, AIS, and CWS. User access is managed by their respective CoSD Program administrators via the NiCE hub. After supervisors set up a user profile, they provide the URL directly to the user. NiCE is a County vendor; all application issues should be referred to CoSD PoC for the respective program. County PoC will open a ticket with vendor. Peraton verifies whether there is a network outage and verifies user headset is functioning; all other issues are referred to the County to engage the vendor.	No	HHSA Coordinated Support
Niche Academy	Niche Academy is an online training tool specifically focused on libraries and the needs of library staff and customers. Tutorials can be developed using simple tools, or existing tutorials developed by the vendor or other libraries can be modified for SDCL use.	Yes	LUEG SaaS Support
No Wait Inside	No Wait Inside allows healthcare providers to invite patients back to their offices without the concern of waiting among other patients that may have a transmittable disease as well as protects their privacy. No Wait Inside is fully HIPAA compliant. Without downloading an app, patients will be able to notify you of their arrival at your facility without calling your staff. When you are ready for them, our tools will notify them that you are ready for them to come in	Yes	HHSA SaaS Support
Northern Trust Custodian Bank	SB272 Public Description	Yes	FG3 SaaS Support
Northpointe COMPAS	Probation Assessment Tool	No	PSG Coordinated Support
OCLC Membership	Acquire OCLC membership and access to all consortium benefits by procuring three modules which will automate and enhance Library operations.	Yes	LUEG SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
OEC Case Management System	The Office of Ethics and Compliance (OEC) investigates allegations of improper county government activity and discrimination based on race, color, religion, sex, national origin, age or disability; and complaints alleging improper County government activity and discrimination. The OEC Case Management System provides a means for OEC to manage Discrimination Complaint Handling and Hotline Call / Web-entry Processing.	No	FG3 Full Support
OES AlertSanDiego Registration	THIS IS A FORM.... Solution which presents on the readysandiego.org Alerts page and which captures registration information securely in both English and Spanish. An American Sign Language delivery option will be available as well as a geocoding capability for registrants.The solution itself will be highly available and will deliver subscription notifications to registrants via email..A secure repository will be maintained in Azure and protect against data loss.	No	PSG Full Support
OES Emergency Map	Modal map showing location of active emergencies (fire, floods, electrical outages, etc.) in San Diego County	No	PSG Coordinated Support
OES Emergency Website	The OES Emergency Websites are SDCOUNTYEMERGENCY.COM, SDCOUNTYRECOVERY.COM, and READYSANDIEGO.ORG. As of 6/19/2019, SDCountyEmergency.com, READYSANDIEGO.ORG, SDCOUNTYRECOVERY.COM have been migrated to AEM.	No	PSG Full Support
OES ENDEC	The Emergency Alert System is a national public warning system commonly used by state and local authorities to deliver important emergency information, such as weather and AMBER alerts, to affected communities over television and radio. The County of San Diego Office of Emergency Services uses the ENDEC system connected to a standalone computer to send emergency alerts to radio station KOGO. The ENDEC EAS system is configured and operated using the ENDEC Pro software installed on a standard desktop PC.	No	PSG Coordinated Support
OES Site Action Plan Form and Repository	eForm and approval workflow process that allows Security Action Plans (SAP) to be created, reviewed, approved, submitted and stored in a central repository for retrieval.	No	PSG Coordinated Support
Ombudsman Data Integration Network (ODIN)	Ombudsman Data Integration Network (ODIN) is a State hosted web application that replaced the CSP Ombudsmanager in October 2013.The Ombudsman Data Integration Network, or ODIN, is a web-based application developed by the Information Technology Bureau and the Office of the State Long-Term Care Ombudsman of the California Department of Aging.ODIN:Tracks facilities, residents, cases, complainants and activities. Generates reports across many variables.	Yes	HHSA SaaS Support
OnBase	OnBase has replaced the application formerly known as ChartOne/ChartVault. It is an ASP hosted by the vendor, Hyland Software, Inc It is a Client/Server model with four main clients that are installed on the County desktop via an MSI.	No	HHSA Coordinated Support
OneLegal	San Diego Superior Court requires the use of One Legal for anye-filings of court documents and, as a result, our legal support staff use One Legal for all e-filings.	Yes	FG3 SaaS Support
Online Trade - Blackrock	This will enable the county to buy and sell Money Market Mutual Funds with Blackrock over their online platform. Currently we can only execute this trade over the phone. No additional products will be traded on this platform.	Yes	FG3 SaaS Support
Online Trade - CalTRUST	The Investment division purchases and/or sells Money Market Funds, (MMF's), on daily basis. The ability to trade and access our accounts online can increase execution efficiency. Treasurer-Tax Collector Investment Officers use this service through a website to access accounts online and process trades.	Yes	FG3 SaaS Support
Online Trade - Federated	This will enable the county to buy and sell Money Market Mutual Funds with Federated over their online platform. Currently we can only execute this trade over the phone. No additional products will be traded on this platform.	Yes	FG3 SaaS Support
Online Trade - Fidelity	This will enable the county to buy and sell Money Market Mutual Funds with Fidelity over their online platform. Currently we can only execute this trade over the phone. No additional products will be traded on this platform.	Yes	FG3 SaaS Support
Online Trade - Morgan Stanley	This will enable the county to buy and sell Money Market Mutual Funds with Morgan Stanley over their online platform. Currently we can only execute this trade over the phone. No additional products will be traded on this platform.	Yes	FG3 SaaS Support
Online Trade - PFM-CAMP	The Investment division purchases and/or sells Money Market Funds, (MMF's), on daily basis. The ability to trade and access our accounts online can increase execution efficiency. Treasurer-Tax Collector Investment Officers use this service through a website to access accounts online and process trades.	Yes	FG3 SaaS Support
Oracle Fusion Middleware	Oracle Fusion Middleware,	No	FG3 Full Support
Oracle Internet Directory (OID)	This is Technology Stack only not an application used for SSO for EBS/FMW/OBIEE.	No	FG3 Full Support
ORCA (Operations Request Coordination Application)	This is a Microsoft Dynamic 365 Cloud application that automates Public Authority business processes. Currently there are 21 departmental operational requests submitted by business unit managers that will be included in the project. The types of requests include: print, facility, employee (new/existing), purchase, IT, miscellaneous, etc..	No	HHSA Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
OverDrive Instant Digital Library Card	Libraries around the United States have been piloting OverDrives instant access Instant Digital Card feature through our award-winning reading app Libby. By adding this powerful engagement tool to your OverDrive services, youre providing potential users instant access to a library card and the eBooks and audiobooks in your digital collection. Offering your community instant library cards is as easy as contacting your OverDrive Account Specialist.	Yes	LUEG SaaS Support
PAR File Online	Online inquiry	No	FG3 Full Support
Parcel Quest	TTC exchanges information and in return get access to use their system/service to get map view of properties.	Yes	FG3 SaaS Support
Partner Engagement System	The Partner Engagement System (PES) is hosted in Microsoft O365 Government Cloud using Dynamics 365 and is a web-based, multi-user application originally built by Microsoft using the CRM Online platform. The PES facilitates the Live Well San Diego partner workflow process from inquiry, onboarding of partner, to ongoing support and communication with the partner. The PES supports internal and external customer service the County collaborates across County groups to engage new partners. Executives and Managers are able to stay up to date with pending and ongoing partnerships through real time, custom reports and dashboards. The PES provides a tool to help the County measure progress of the Live Well San Diego vision through the collective impact of partner activities and outcomes that are linked to the Areas of Influence and Indicators. The PES does not contain any customer/client data; however, it does contain data about Live Well San Diego County partner organizations (i.e., name of entity, entity POC, entity location, sector, reach, commitments to further the LWSD vision & outcomes). Each partner reports information about actions their organization is taking in support of CoSD's Live Well initiatives which is later included in LWSD Annual Report published to the public. The addition of Dynamics 365 Portal provides limited partner access to enable more real-time reporting and contains a knowledge base managed (e.g., data entered) by the County. Application is fully supported by Perspecta.	No	HHSA Full Support
PARTS - Public Authority Registry Tracking System	The PARTS (Pubic Authority Registry Tracking System) application will manage the providers and consumers for IHSS Public Authority.	No	HHSA Full Support
PatternStream	The new Pattern Stream Automated Documents System (PADS) allows users to rapidly set up, test, modify, run, and save automated publishing projects. Information can be acquired quickly from a standard database, XML and HTML files, as well as other files. PADS generates Adobe FrameMaker, Postscript, and Acrobat files as output for electronic distribution and print. PADS is accessed via Terminal Services (or Remote Desktop) as a desktop application that sits on an AWS EC2 instance, ec2padswp014374. All supporting applications that are needed to support PADS reside on ec2padswp014374 (i.e., MS Office, Adobe FrameMaker, and Acrobat).	No	FG3 Coordinated Support
PCC Staffing Database	Access Database used for tracking staff at PCC, including training, assignments and scheduling.	No	HHSA Coordinated Support
PDS Mobile Building Inspection	PDS Mobile Building Inspection App is one of the CityGov Apps related to Accela	No	LUEG Coordinated Support
PeachJar (DCSS)	PeachJar is a digital flyer management system. It is a cloud based platform for school districts around San Diego County to deploy and manage digital flyer approval and delivery to parents.	Yes	PSG SaaS Support
PeopleSoft HCM	County of San Diego PeopleSoft application for Payroll, HR, Benefits and ePerformance	No	FG3 Full Support
Performance Budgeting	The CGI Advantage Performance Budgeting system is the budgeting system for CoSD. Performance Budgeting replaced PA1089 BRASS system in 2013.	No	FG3 Coordinated Support
Performance-based Standards (Pbs)	Performance-based Standards (Pbs) allows agencies to collect measurements around safety, security, order, health and mental health, justice, programming, reintegration, and family/social supports. This will allow each of our three facilities to independently track their progress and outcomes in all areas of operations and support.	Yes	PSG SaaS Support
Periscope	Social Media Video Integration with Twitter	Yes	FG3 SaaS Support
Persimmony	"Persimmonys Electronic Case Management and Targeted Case Management Solution is designed to support client care, client monitoring, time study reporting, and TCM billing including MAA and Medi-Cal interfaces.	Yes	HHSA SaaS Support
PG Pro Web	Fiduciary/Trust Accounting	Yes	HHSA SaaS Support
Pharmacy DicksonOne Data Logger	DicksonOne DataLogger is a third-party, vendor supported proprietary Cloud-based SaaS application used by the Pharmacy department to monitor and record real-time temperatures and other critical parameters related to analytical and diagnostic testing. Continuous temperature monitoring and documentation is required by regulatory agencies for equipment used to store patient samples, test kits, reagents, and supplies. Monitored equipment includes refrigerators, freezers, water baths, and incubators. This monitoring system continuously monitors and records temperature and humidity readings and sends real-time malfunction alerts to County staff. It is also used by the County Immunization department (CA6219) and the PHL Telemetry department (PA2819). Data logging devices are on a VLAN located at Site 33.1.	No	HHSA Coordinated Support
PHPR San Diego Healthcare Disaster Coalition Public Website	The Public Health Preparedness and Response (PHPR) Branch coordinates with emergency management agencies, community organizations, medical providers, prehospital provider agencies (fire/EMS), hospitals, clinics, skilled nursing facilities, businesses and other partners in developing public health and disaster preparedness.	No	HHSA Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
PHS Immunization Online Appointment System	PHS Immunization Online Appointment System allows public health centers to provide an online appointment system for the public to schedule their immunizations online. Diseases like whooping cough, chickenpox, and pneumonia are still very common and can be very serious. These infections can spread in daycare and school. It is also very important for adolescents between 11-18 years of age to receive vaccines to prevent whooping cough (the Tdap vaccine), meningitis (meningococcal vaccine), and cancer (HPV vaccine). All adults need a whooping cough vaccine and many adults also need vaccines to prevent pneumonia, hepatitis, and flu. The PHS Immunization Online Appointment System improves patient satisfaction and grants easier access to immunization services. It alleviates long wait times (without any guarantee of being seen on the same day) at public health centers for vaccinations.	No	HHSA Coordinated Support
Pictometry	Aerial imagery for San Diego County	Yes	FG3 SaaS Support
Picture Archiving Communication System (PACS)	Integrates the CoSD vendor Quick Study Radiology, Inc's. Picture Archiving Communication System (PACS) hardware and software service offering with the County of San Diego's network observing both the CoSD security and standards for data protection. This will allow off-site storage and separate disaster recovery storage.	No	PSG Coordinated Support
Piktochart	The application stores powerpoint type information created by staff who have purchased the piktochart software. The data is shown as dashboards that consist of statistics and cost for various programs/projects. Used for creating dashboard presentations.	Yes	PSG SaaS Support
Pinterest	Social Media Site	Yes	FG3 SaaS Support
Placement Coordinator Office Database	The Placement Coordinator Office Database application supports the HHSA Child Welfare Services group in tracking information related to foster homes. Information related to foster homes includes: general contact information, clearances, holds, trainings attended, etc.	No	HHSA Full Support
PolicyTech	PolicyTech Software manages HHSA Public Health Services policies and procedures (P&Ps). The PolicyTech Software is hosted at PolicyTech, Inc. servers. The users access the PolicyTech Software via the internet. No sensitive or confidential data will be stored in the system.	No	HHSA Coordinated Support
Polinsky Donor Tracking System	This application is used by Polinsky and tracks Donations, this is a MS access application, the data base technology also MS access	No	HHSA Coordinated Support
Polinsky Kids Information Data System	Polinsky Childrens Center tracking system.Tracks and collects information on children who were admitted to Polinsky.	No	HHSA Full Support
PollEverywhere	Poll Everywhere transforms one-sided presentations into two-way conversations with the audience. This web-based audience response system lets you embed interactive activities directly into your presentation. The audience responds on the web or via SMS texting on their phones.	Yes	HHSA SaaS Support
Powtoon	Founded in 2012, Powtoon is the most user-friendly and intuitive animation software. With Powtoon, you can create engaging, animated videos with a professional look and feel. Powtoon has roughly over 16 million users worldwide and over 45 million Powtoons have been created and shared around the world.	Yes	PSG SaaS Support
Precinct Activity Tracking System	ROV/Maps and Polls uses PATS to track precinct boundary changes. All changes are manually inputted and accessed by Crystal Reports for State reporting purposes. The reports are generally sent prior to each major election following a request.	No	FG3 Full Support
Prezi Presentation	"Prezi is a cloud-based presentation software and storytelling tool that will be used for presenting ideas on a virtual canvas. The product employs a Zooming User Interface, which allows users to zoom in and out of their presentation media, and allows users to display and navigate through information within a 2.5D or parallax 3D space on the Z-axis.Prezi is a cloud-based presentation software and storytelling tool that will be used for presenting ideas on a virtual canvas. The product employs a Zooming User Interface, which allows users to zoom in and out of their presentation media, and allows users to display and navigate through information within a 2.5D or parallax 3D space on the Z-axis. Prezi will allow staff to create dynamic presentations. Prezi is the only presentation application of its kind that allows users to create animated, visually engaging presentations. This software will be utilized by staff to present engaging presentations on County services/programs to internal County employees, contractors and the community.	Yes	FG3 SaaS Support
Probation Case Management System (PCMS)	The San Diego County Probation Department is responsible for supervising clients referred to or granted probation by the Court. Probation Case Management System (PCMS) maintains records for all clients' cases assigned to the probation department.	No	PSG Coordinated Support
Probation Contact Log Mobile Application (PUMA)	Probation Mobility App a.k.a Puma helps Probation Officers to conduct their everyday business when they visit Probationers (both Juvenile and Adults). PUMA stands for Probation Utility Mobile Applcations	No	PSG Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Probation Electronic Medical Records (PEMR)	The Probation Electronic Medical Record (PEMR) is a web-based correctional medical records system that provides for comprehensive correctional medical practice management, tracking every activity related to an inmate's healthcare, streamlining the complex workflow, providing practical efficiencies and easy access to inmate health records via a user-friendly, dynamic and intuitive interface.A medical record is generated at the time of booking. There are about 650 to 800 minors (children under 18 years of age) in the system at any given time. Some of those minors have been in the system more than once but they keep the same Medical Record number (MR#) for life. The retention time for medical records is 10 years. After the age of 18, their records are boxed up and stored at Iron Mountain. Those records will be destroyed after 10 years. Upon launching the PEMR system, there will be approximately 625 active Medical Records in the system. There are some records kept in the system for probationers that are over the age 18. It can receive and store records for probationers up to age 21.Each Medical Record contains approximately 10 standardized forms, plus the documentation from the providers that accompany them. Depending on the kids' length of stay, health problems and times that they have been in and out of the system, there are typically 1 to 4 volumes of Medical Records and of which some can go up to 6 volumes. (A volume can be several inches thick of paper.)	No	PSG Coordinated Support
Probe Information Services Inc - Investigative Srvs	Probe Information Services, Inc. The vendor will receive a request that includes personal identifiable information and medical information; this information will be entered into their system in order to perform the services requested and then provide a report (that contains such information), which may include video.	Yes	FG3 SaaS Support
Progen	Construction Project Management Application	No	FG3 Coordinated Support
Progen	This application is provided to DGS as a component of a construction consulting contract. The application is not contracted for separately, but is a tool used by the vendor to provide their services. The Department of General Services (DGS) utilizes the Gordian Group for the maintenance and administration of its JOC program. Support from the Gordian Group includes publication of the Unit Price Book (Construction Task Catalog), monitoring of local area construction pricing used by the County, permission to use their licensed proprietary software system (PROGEN), technical support as well as construction management training to all County and Contractor employees, and a full range of system management services throughout the entire JOC process.DGS Project Management Division uses the PROGEN product as a project and contract management system for the JOC program. PROGEN functions includes: Trackso Job Order Contract (JOC) amounto Project numbero Contract numbero Contract amounto Contractoro Contractor information (address, phone number, email)o Facility addresses	Yes	FG3 SaaS Support
Project Clean Water Website	This contract is to obtain expert consultant services to support and maintain the existing Project Clean Water website. The Regional Water Quality Control Board requires the County of San Diego, and other parties listed under the MS4 Permit (Order No. R9-2013-0001), to develop, update and maintain an internet based Regional Clearinghouse that is made available to the public. The Project Clean Water website currently serves as the Regional Clearinghouse for the County of San Diego and other parties under the MS4 Permit. The website provides required public access to water quality data, map layers, plans, reports, and other documents and files.	Yes	LUEG SaaS Support
Prop 60/90/110	Exemption for senior citizens and disabled folks. Application hosted in Citrix environment and accessed using the Citrix link in the Hosted Websites section.	No	FG3 Coordinated Support
Prop 8	Tracking and mailing system	No	FG3 Full Support
Property Parcel Corrections Database	UNK	No	FG3 Coordinated Support
Proscript	Pharmacy system for Edgemoor Hospital. The Appication was developed by Prodigy Data Systems in Alberta, CA (http://ProdigyDataSystems.com/) and also includes HermeTech EasyHL7 TCP/IP Services. This application is a client application that runs inside of Citrix and accesses a database located on the same server as this application.	No	HHSA Full Support
PSG Inventory Management System (Maximo)	Maximo or PSG Inventory Management System (PSG-IMS) is an inventory management solution for assets, supplies, and safety equipment used by the San Diego County Fire Authority (SDCFA) and the Office of Emergency Services (OES). Currently, only 2 of the 11 departments within PSG are migrating their papers systems to this standard system. The intent is that all PSG departments will be using this standard Inventory Management System in the future.	No	PSG Coordinated Support
Public Access to Court Electronic Records (PACER)	This is classified as a service. TTC Users are able to access, search, and view the bankruptcy case activity maintained by the Federal Bankruptcy Court. TTC submits claims electronically to the Federal Bankruptcy Court. Access to this site must be obtained directly from the vendor pursuant to vendors terms of service, agreement and fees.	Yes	FG3 SaaS Support
Public Defender eShare	Sharepoint 2010 farm for management of Public Defender electronic content. Note: Patching to this app requires that the database be taken out of high availability mode.	No	PSG Full Support
Public Health Information System (PHIS)	Public Health Services case management/ claiming system. The Public Health InformationSystem runs on an Intel web server running Windows Server and an application/database SUN/Oracle server running Solaris. The application that runs on the application server is myAvatar by NetSmart (http://www.ntsd.com/) and the database is Cache by InterSystems (http://www.InterSystems.com/).	No	HHSA Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Public Health Lab Telemetry	DicksonOne DataLogger is a third-party, vendor supported proprietary Cloud-based SaaS application used by Public Health Lab (PHL) Telemetry department to monitor and record real-time temperatures and other critical parameters related to analytical and diagnostic testing. Continuous temperature monitoring and documentation is required by regulatory agencies for equipment used to store patient samples, test kits, reagents, and supplies. Monitored equipment includes refrigerators, freezers, water baths, and incubators. This monitoring system continuously monitors and records temperature and humidity readings and sends real-time malfunction alerts to County staff. It is also used by the County Immunization department (CA6219) and the Pharmacy department (PA2816). Data logging devices are on a VLAN located at Site 33.1.	No	HHSA Coordinated Support
PulsePoint AED	PulsePoint AED is a simple-to-use app that enables you to help build the public AED registry in your community or anywhere! When a cardiac emergency strikes, finding an Automated External Defibrillator (AED) can help save a life. But that takes knowing where AEDs are located.AEDs that are managed using PulsePoint AED are accessible to emergency dispatchers and disclosed to emergency responders, including nearby citizens trained in CPR and off-duty professionals such as firefighters, paramedics, and nurses. Instead of asking the caller if there is an AED available, dispatch center staff can inform callers of nearby lifesaving devices.There is never a charge to use any aspect of the PulsePoint registry. PulsePoint is a public, non-profit organization providing the app and hosted AED registry for free as part of its core mission to improve cardiac arrest survival. Lets save some lives together.	Yes	PSG SaaS Support
Purchasing and Contracting Documentum Repository	Documentum is the system of record for all documents related to contracts and purchase orders for the County of San Diego. The Purchasing and Contracts Records Application was created to provide a user-friendly means for importing, searching and retrieving these documents. In addition, County employees and the public may search and view content based on permissions established by the department. The Purchasing and Contracting Records Application consists of the following areas of functionality: 1) The EDPP Enterprise Documentum Platform based on Documentum 2) ImageTrust for scanning 3) A custom web-viewer that allows users to import and search for documents based on user permissions. 4) An interface with EBS (Oracle Financials PA2150) to integrate viewing, and indexing 5) Leveraging the new County Website standard, Adobe AEM to provide internally and externally facing access to content The Purchasing and Contracting Records Application content resides within the COSDGEN Repository in Documentum.	No	FG3 Coordinated Support
Pyxis	The Pyxis Med-stations from Becton Dickinson, CareFusion division are being used by Health and Human Services Agency (HHSA) San Diego County Psychiatric Hospital (SDCPH) for inpatient services. The Pyxis medication cart dispensing system will automate aspects of SDCPH's medication process including dispensing patient medication, provide the ability to monitor medication stock levels thereby ensuring availability of medications, while reducing overstocking (daily inventory reconciliation are accurate). Pyxis will interface with PA2732-Cerner Millennium RHO and receive patient ADT (Admission, Discharge and Transfer) Orders, and receive medication orders from Cerner Millennium and dispense medications for SDCPH through Pyxis, with the goal of reducing medication errors and provide for the means to dispense medications outside of normal Pharmacist hours. The Pyxis system is vendor supported.	No	HHSA Coordinated Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Pyxis Knowledge Portal	SDCPH Pharmacy desires to upgrade its 4 of its current Pyxis 4000 Medstation to the Pyxis ES Platform. By upgrading to this platform solution, SDCPH Pharmacy will have access to BD's Knowledge Portal. Knowledge Portal is an intuitive, web-based application that quickly translates data into actionable information. Data and key performance indicators (KPIs) can be accessed with just a few clicks to help optimize devices and standardize hospital policies, without data overload or additional manual steps.The Pyxis ES solution is a 3rd party solution that is managed by the vendor within a 3rd party isolated VLAN in Rosescrans, SD. The Knbwledge Portal solution is a cloud hosted solution in the SuperNap Datacenter in Las Vegas, NV. There are many advantages for SDCPH Pharmacy to upgrade to the Pyxis ES Platform Solutions and thus obtain access to the Knowledge Portal which comes standard with the solutions. See below for details:1) The records retention feature is primary, plus having data in one area instead of a hybrid. - The current data is stored in Perspecta's environment. Once 30 days had passed, Perspecta's server does not allow useable information in a readable format, therefore putting SDCPH Pharmacy at risk in the event of audit.- In the Knowledge Portal platform, records retention is up to 10 years2) Another benefit with the platform upgrade, it will come with software upgrades as the current platform is discontinued. Newer software has a patient centric approach which should decrease med errors and increase patient safety. 3) Medication management integration with Cerner Millennium (SDCPH's current Electronic Health Records system) - There is an interface built between the two so that medication info can be transferred back and forth.- The Pyxis ES Platform integrates with the Cerner Millennium system itself and various applications such as Discern Analytics, PowerChart, PharmNet, so pharmacists can draw upon this medication dispensing data	Yes	HHSA SaaS Support
Q Continuum System	Q is a HIPAA compliant, Internet-based tool for client centric, data reporting. This application is used by AIS staff in numerous programs. The tool is used for assessments, care plans and logging services. Information about individual consumers is shared within the provider network. This application serves as a "data warehouse" for data that crosses numerous AIS support programs.	No	HHSA Coordinated Support
Qmatic - Clerk of the Board	This application is used by customers to schedule Passport Appointments online and then the Clerk of the Board Passport Office employees use the application to manage the appointments once the customer enters the building.	No	FG3 Full Support
Q-MATIC ARCC	The ARCC offices use Q-MATIC Orchestra to manage a queue of customers via system created tickets. Customers are given a printed ticket or mobile text which is called to service counters via audio PA system, video queue display TV monitors, mobile text, mobile app, and/or on service counter LED where the ticket is being served. Q-MATIC saves ticket service information, allowing the generation of reports showing service performance, wait times etc. Customers can also schedule appointments via an online appointment web interface. Appointment confirmation emails are sent to the person who scheduled the appointment. The system is live at all ARCC County sites.	No	FG3 Coordinated Support
Q-Matic COB	Q-Matic is a queuing system to manage Clerk of the Board passport customers. Q-Matic will be providing the Orchestra software via a cloud solution.	Yes	FG3 SaaS Support
Q-Matic HHSA EO	Client Visit Management (CVM) is shared by the FRCs with the ability to handle minor differences between the sites. Some of the functionalities are: 1. Appointment / Check-in,2. New application, 3. Orientation and 4. Other (AKA: Q-Matic).	No	HHSA Full Support
Q-Matic LUEG	Line Queue Management... Customer Flow Management System - used for customer intake, routing customers to the appropriate LUEG permitting counter (e.g. DPLU, DEH, or DPW) and capturing actions conducted by staff for customers. Includes QSuite and Management Portal software with the following optional modules: Calendaring and SDK Wait Times. The public-facing application displays wait times for permitting services at Site 5 and allows the public to schedule appointments.	No	LUEG Coordinated Support
Qualtrax	Qualtrax is a compliance management software for the forensic industry. It centralize auditable data into a single web-based interface, automate required processes for equipment calibration, purchase requests, customer complaints and more.	Yes	HHSA SaaS Support
Qualtrics 360 Basic	Develop high-performing employees and stronger teams with 360-degree feedback insights that drive development, productivity and engagement.Automate the process of multi-rater reviews with faster, simpler feedback.Empower managers to hold more actionable conversations based on trends and analysis from 360° data.Deliver individualized reports to employees and protect raters anonymity with built-in confidentiality features.Launch expert-designed 360 assessments in minutes, with pre-built surveys and programs straight out of the box. Give managers instant feedback about their direct reports, get real-time progress updates to see which raters have completed their reviews, and access customized task lists.Quickly and easily see where to focus your efforts to develop your top performers. Managers receive real-time reports identifying strengths and areas for improvement for each team member. Plus, with built-in action planning, they have the tools they need to turn data into improvements and help their direct reports develop their skills.	Yes	HHSA SaaS Support
Quest Quanum Lab Services	Quanum streamlines requests and review of lab testing.	Yes	HHSA SaaS Support
QuickBooks Online	QuickBooks is an accounting software package developed and marketed by Intuit.	Yes	HHSA SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Rad Responder	The RadResponder Network is the national standard and Whole Community solution for the management of radiological data. It is a product of collaboration between Federal Emergency Management Agency (FEMA), Department of Energy (DOE) / National Nuclear Security Administration (NNSA), and the Environmental Protection Agency (EPA), and is provided free of charge to all Federal, state, local, tribal, and territorial response organizations.The application will be accessed via the browser and a mobile app.	Yes	PSG SaaS Support
Random Moment Timekeeping System (RMS)	The system tracks Title IVE hours that the Probation Officer spends on a particular case.	Yes	PSG SaaS Support
Recorder Vital Records System	Recorder system for managing vital record indexes, on-line display and issue Certified Abstract copies	No	FG3 Full Support
Red Arrow	DHR Medical Standards Unit utilizes this application to administer the mandatory Federal Omnibus and random drug/alcohol testing programs county-wide.	Yes	FG3 SaaS Support
Redemption (Prior Year/Secured/Defaulted) Taxes	Post payments and penalties; make changes/updates, generate reports; provide on-line access; print Tax Bills (both production Enterprise and On-Demand at remote printers); downlaid mini-database to TAPPIS; generate electronic media for Tax Agencies.	No	FG3 Full Support
Rental Mobile Home DB	Assessors tool to track rental mobile homes	No	FG3 Coordinated Support
Representative Payee (Foster Care)	Application to manage claims check for Fostercare program	Yes	HHSA SaaS Support
Revenue and Recovery State Reports	Revenue and Recovery State Reports, external program installed on County desktops	No	FG3 Full Support
RJN Inc. - Investigative Services	RJN InvestigationsThe vendor will receive a request that includes personal identifiable information and medical information; this information will be entered into their system in order to perform the services requested and then provide a report (that contains such information), which may include video.	Yes	FG3 SaaS Support
Robotics	Robotics is used to audit data which is obtained from Oracle, PeopleSoft and US Bank.	No	FG3 Coordinated Support
ROV AEM Website (SDVOTE.COM)	ROV AEM website WWW.SDVOTE.COM on Adobe Experience Manager Platform.	No	FG3 Full Support
ROV Bulk Email	The Registrar of Voters (ROV) group currently uses the Outlook client which calls macros to collect sender information and send bulk emails to UOCAVA and SBOPTOUT users. Internal Email routes to the Office 365 internal connector and external Email uses cloud-based partner connector, Cisco IronPort. However, Office 365 won't allow bulk e-mail of more than 10,000. ROV needs a solution that can support more than 10,000 e-mails at once. The solution is to use a third party tool, SendGrid, to send bulk emails and upgrade the current macros to a modern computer programming language, a .NET application that connects to SendGrid.	No	FG3 Coordinated Support
ROV Documentum Generic File Cabinet	The ROV Generic File Cabinet was established to provide a central place to store an access documents. Users import and access content directly through CARA Another application ROV dashboard also associated with this PAID. This dashboard created to search and view ROV microfiche documents i.e. affidavits and index documents.	No	FG3 Full Support
RSVP Volunteer Reporter	Volunteer db used by Aging and Independent.	No	HHSA Coordinated Support
San Diego Air Pollution Control District Home Page	Public facing Web presence for San Diego Air Pollution Control District Website serving residents and visitors of San Diego County.	No	Other Full Support
San Diego Air Quality Complaints	Mobile Application for reporting of air quality complaints such as Odor, Smoke, Dust, Asbestos, within San Diego County.	No	Other Coordinated Support
San Diego Childhood Obesity Initiative Website	The San Diego County Childhood Obesity Initiative is a multi-sector coalition with the mission of reducing and preventing childhood obesity by advancing policy, systems, and environmental change through collective impact.	Yes	HHSA SaaS Support
San Diego County Park Reservation System	This is the County's Park Reservations System that enables members of the public to reserve camping spots in County's Parks.	Yes	LUEG SaaS Support
San Diego County Property Reutilization	This hosted web based application allows internal County Depts. to offer surplus goods to other internal County Depts.via web site. This service is incidental to the overall Auction Marketing Contract.	Yes	FG3 SaaS Support
San Diego Immunization Registry	Provides central point for immunization records for county individuals	No	HHSA Full Support
San Diego Risk & Resiliency Checkup (for CBO)	The San Diego Risk & Resiliency Checkup (SDRRC), is an evidence based juvenile offender risk/needs assessment tool. Community Based Organizations (CBOs) will be using the web-based version of the tool to complete an assessment of selected clients. The SDRRC will provide the CBOs with information related to a youth's level of risk to re-offend, identify criminogenic need, develop meaningful case plans, and be used to monitor progress in reducing criminogenic needs. SDRRC provides several essential upgrades from a current version of the SDRRC web-based juvenile assessment tool that the CBOs have been using since 1998.	No	PSG Coordinated Support
SD Emergency Mobile Application	The County of San Diego Office of Emergency Services (OES) created the SD Emergency app to better prepare and inform San Diego County residents and visitors about disasters. With SD Emergency, the tools you need to plan, prepare and respond in an emergency are right at your fingertips.	No	PSG Full Support
SDE Repository	Enterprise geodatabase is configured on SDEP and SDEP2 databases in New Tulsa. PA2350 also interfaces with SanGIS FTP for data refresh via ADR G4 application. Related PA2005 contains REST\API map layers.	No	LUEG Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
SDFood Info	CityGov Application: DEH provides food facility information to the public via the Eat Safe application. The Eat Safe responsive website will provide the dates of inspections at food facilities in San Diego county, as well as related findings during these inspections. The website includes an interface the provides both tabular data and a map of food facilities.	No	LUEG Coordinated Support
SDPARKS AEM Website (www.sdparks.org)	www.SDPARKS.org AEM website on Adobe Experience Manager Platform.	No	LUEG Full Support
Secure Web Drop Box	Used to securely transfer confidential files or large files (<10MB) with external organizations	No	FG3 Coordinated Support
Selectron IVR	The Selectron Systems assists County Residents who call in on the PDS phones number reach the people who can provide them with the services they need. The Selectron system which is hosted as a SaaS application can route callers, schedule services and deliver needed canned information. With the latest release SelecTXT feature was added to the system which allows users to quickly and easily interact with your agency via SMS text messaging.	No	LUEG Full Support
Sempra Energy EDT	Sempra EDT support for the 2021 Emergency Rental Assistance Program (ERAP), a Federally and State mandated program which falls under the Consolidation Appropriations Act signed by Congress in December 2020 to provide housing relief to victims of COVID-19. San Diego County residents seeking rental and utility payment assistance submit applications through PA2825 CoSD COVID-19 Emergency Rental Assistance Program 2021. Housing and Community Development Services (HCDS) staff will determine eligibility and process payments by confirming account information and accuracy with SDG&E. The validation will be completed through SDG&Es SFTP site.	Yes	HHSA SaaS Support
Sentinel	Global Positioning System(GPS) for Ankle Bracelet and Juvenile Breath Alcohol Real-Time(BA-RT remote deep lung alcohol testing).	Yes	PSG SaaS Support
Sentri7 Real Time Clinical Surveillance	Designed by clinical experts. Controlled by pharmacy and infection prevention teams. Improving a program's performance relies on busy care and teams receiving the necessary tools and knowledge within their daily workflows. Sentri7® clinical surveillance aggregates EHR data to prioritize and alert care teams in real-time. By delivering earlier evidence-based interventions, your hospital can make a bigger impact on patient outcomes.	Yes	HHSA SaaS Support
ShakeReadySD	Earthquake early warning system based on alerts from USGS and sent to subscriber's mobile phones.	No	PSG Full Support
SharePoint O365 Platform	SharePoint Online O365 (Enterprise SharePoint Online Platform in Office 365)	No	FG3 Full Support
Sharpe IPM	SharpeSoft IPM (Integrated Project Management) for construction contract management; Modules include estimating, bid management, inspector dailies, T&M, and progress pay estimates. Customer need to be in rApp-SharpeIPMCtxUsers to see the Sharpe published app when they log onto the Citrix environment. G_App_CitrixReceiver_ENT_EVUM_SCCM is the group they need to be put in to get the Citrix receiver pushed to their machine.	No	LUEG Coordinated Support
Sign Up Genius	An online software tool for volunteer management and event planning.	Yes	HHSA SaaS Support
Siteimprove	Scanning and reporting tool for web content. This tool will provide reporting on where our website is not meeting accessibility standards (WCAG/508/ADA) as well as providing reports on broken links, misspellings and other site quality information. Modules purchased:Quality AssurancePolicyAccessibilitySearch Engine OptimizationResponse For more details go to www.siteimprove.com	Yes	FG3 SaaS Support
Skedda	Skedda is a cloud based subscription which allows a CoSD to reserve desk space.	Yes	PSG SaaS Support
Slack	Overview: The San Diego County Public Health Services and Office of Emergency Services formed a network (Partner Relay) to share information with Limited English Proficient communities during emergencies. The communities included those who spoke Spanish, Tagalog, Chinese, Korean, Arabic, Vietnamese, Somali, and Karen.Translation Requests:As Emergency Public Information Updates are posted to www.SDCountyEmergency.com, these posts will be automatically added to a specific www.Slack.com channel (username/password required) for the community partners to translate and then disseminate to their communities. Additionally, there will be coordination from County staff at the Emergency Operations Center to the Partner Relay through Slack.There are around 300 participants in the Partner Relay.At this time, the Partner Relay will use the free version of Slack.	Yes	PSG SaaS Support
Small Business Grants Portal	The Small Business Grants Portal is a Power Apps application where San Diego county small businesses can apply for a business grant and that application can be tracked throughout the process.	No	FG3 Full Support
Smart Horizons - Career Online High School	Smart Horizons Career Online High School (COHS) offers career-based online high school programs to serve the millions of adults and older youths who have dropped out of high school. Our programs are designed to prepare students to enter or advance in the workplace, and include career certificate.	Yes	LUEG SaaS Support
Smartsheet	Smartsheet is a software as a service (SaaS) application for collaboration and work management that is developed and marketed by Smartsheet Inc. It is used to assign tasks, track project progress, manage calendars, share documents, and manage other work. It has a spreadsheet-like user interface. OSI intends to use Smartsheets as a productivity tool to manage and communicate with teams involved in the numerous events and projects managed by the Live Well San Diego Support Team. Teams include county and non-county employees, community volunteers, and county contractors.	Yes	HHSA SaaS Support
Snapchat	Social Media Site	Yes	FG3 SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
SOCAT	State Application for County Expense Claim submission	No	HHSA Coordinated Support
Social Press Kit	This will be used to create toolkits around board letters and encourage orgs/community members to be involved and share their support.	Yes	FG3 SaaS Support
Special Assessments by Parcel Number Search	Displays special assessments by parcel number	No	FG3 Coordinated Support
Specialized Investigations, Investigative Services	Specialized Investigations, Inc.The vendor will receive a request that includes personal identifiable information and medical information; this information will be entered into their system in order to perform the services requested and then provide a report (that contains such information), which may include video.	Yes	FG3 SaaS Support
SPSS	This PAID is to support the SPSS licensing server only. SPSS is a Desktop application, obtained through the CoSD Service Catalog. It is an analytical software that provides analysts with the foundation for project planning, data collection, data access, data management and preparation, data analysis, reporting and deployment. Application issues, such as driver installation or load to the user's desktop, are managed by Desktop Support.	No	HHSA Coordinated Support
SquareSpace	Blog site for county news and employees can post blogs	Yes	FG3 SaaS Support
StarLIMS - Web	Web based Laboratory Information Management System installed in the San Diego County Public Health Laboratory on Rosecrans. This Application also uses the "Batch Scanning" process to scan the requisition forms that need to be uploaded to StarLims. This Application also uses an AEM eForm for 3rd party request of Laboratory specimen testing. This Application can import a specific formatted CSV file with patient data which is currently in use by Healthbook (in SNOW). STARLIMS provides laboratory specimen testing and result reporting data management. Application can import a specific formatted CSV file with patient data which is currently in use by Healthbook (in SNOW).	No	HHSA Full Support
Statewide Automated Reconciliation System (SARS)	The SARS Statewide Automated Reconciliation System provides reports and data related to EBT benefits and EBT Cards issuances and usage. The site is maintained by State Office of Systems Integration EBT Project. San Diego County utilizes SARS to obtain EBT data related to state mandated reports. Fiscal utilizes SARS data related to monthly reconciliation reports. This is a state mandated site and is maintained by the state. San Diego staff accessing the SARS site are assigned unique User IDs and create their own passwords. See attached County Fiscal Letter 01/02-62 issued by the state on 9/16/2002 for additional details.	Yes	HHSA SaaS Support
StormWater App	Stormwater app is an inspection app built by CityGovApp. Inspectors use the app to enforce stormwater laws and regulations at commercial agricultural operations in the unincorporated area of San Diego County.	No	LUEG Coordinated Support
Streamline	STREAMLINE automation system provides a specialized fire inspection management solution. It is a mobile and cloud based inspection platform created for state and local governments.	Yes	PSG SaaS Support
StreetSaver	A condition management system for County maintained road.	Yes	LUEG SaaS Support
Submeter Lab App – Inspections and Work-log	Submeter Inspections and Work-log is one of two apps by CityGovApp app created to reduce the amount of time it takes for customer check-in, inspector stocking, testing, sealing, customer check-out, and payments of water, vapor, and electric submeters. (The other app is Submeter Check-in and Check-out)	No	LUEG Coordinated Support
Submeter Lab App-Check In & Check Out	Submeter Check-in and Check-out is one of two apps by CityGovApp app created to reduce the amount of time it takes for customer check-in, inspector stocking, testing, sealing, customer check-out, and payments of water, vapor, and electric submeters. (The other app is Submeter Inspections and Work-log)	No	LUEG Coordinated Support
Summer Learning Solution	READsquared is the premier Reading Program and Readers Advisory Service on the market, un-matched in its ability to customize, extend, and promote your librarys unique brand. http://www.readsquared.com/	Yes	LUEG SaaS Support
Supplemental Online	Online inquiry	No	FG3 Full Support
Survey Records System	The Survey Records section business mission is to provide easy to use searchable systems for researching various maps, control monuments, survey data, and survey documents related to the County Surveyor functions. The current Survey Records System (SRS) was created in 2002 to provide an online system to meet the business mission needs. The technology of current system has become antiquated over the past decade. DPW is looking for a replacement with modern technology that is robust, easily accessible from multiple platforms, and easy to maintain.	No	LUEG Coordinated Support
SurveyMonkey Enterprise	Survey Monkey is an online application that allows users to create surveys, send surveys to a targeted audience, track responses, and analyze the results of the surveys. Its user friendly interface allows users to obtain the Voice of the Customer which helps the Agency assess and improve internal processes and critical services that are provided to our customers.	Yes	FG3 SaaS Support
Tableau Online	Tableau Online is an analytics platform fully hosted in the cloud to publish dashboards and interactive visualizations of data. These will be accessible from a browser or with Tableau mobile apps.	Yes	HHSA SaaS Support
Taser/Axon Evidence Sync	Probation Officers are equipped with Taser Electronic (smart) Weapons. Evidence Sync supports these tasers by updates to firmware, perform basic diagnostics and download Conducted Electrical Weapon (CEW) events. CEW event reports are an important liability protection, they protect the County against exaggerated claims related to use of force. The Evidence.com site will store: Officer Name, CEW Serial #, in the event of two officers with same name a Date-of-birth may also be stored.	Yes	PSG SaaS Support
Tax Rate by Tax Rate Area Search	Tax Rate by Tax Rate Area Search -- Web Application	No	FG3 Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
TB - Fujifilm	The County of San Diego (CoSD) Public Health Services Tuberculosis (TB) clinic performs approximately 3,000 chest radiographs annually or approximately 15 per day for the TB clinic combined with the mobile van (note: as of spring 2022 the TB clinic has been operating from the mobile van due to structural issues at the Rosecrans facility. The users moved out, but the physical servers remain at Rosecrans. The new clinic location has not been identified.) TB Control uses Fujifilm's medical imaging and information management system, Synapse Picture Archiving and Communication System (PACS), to capture, review, and archive x-ray images in its radiology suite. This standalone 3rd party solution resides in a Virtual Circuit at the Rosecrans County Health Services TB Clinic (Site 33). At Rosecrans there is a Fuji Physical Server (ESXi host) and NAS Device (Iomega). The ESXi hosts 2 virtual servers - Test and Prod.	No	HHSA Full Support
TeamMate	The Teammate software package is used to facilitate internal CoSD audits conducted by the Office of Audits and Advisory Services (OAAS). All findings, recommendation and associated workpapers related to the audit are held in the application.	Yes	FG3 SaaS Support
TellUsNow	CityGov Mobile Application (Android and IOS)	No	LUEG Coordinated Support
Tenex-Live Results	Provide Election Results - SaaS - Third Party Vendor Tenex. Use Third Party solution to provide Election Results. The Registrar of Voters needs to provide unofficial election results on election night every 30-60 minutes. These results are provided to the public, the media, and officials at Golden Hall. The Tenex solution, Live Results, deliver election results to the public that are easy to navigate, delivers results down to the precinct level results, and provides intuitive maps and graphs of federal, state and local elections.	No	FG3 Full Support
TotalLearning Management System	Learning Management System for Employee Training which is access via URL https://cosd.sumtotal.host/core. This application is hosted in the cloud by SumTotals, LLC	No	FG3 Coordinated Support
Tran Control Log: Shrink Wrap	Tracking Database. Used by Assessor Clerks in Mapping Division to track non-taxable agencies	No	FG3 Coordinated Support
Transform for CalWIN Checks/Warrants	The county of San Diego uses the Transform tool as one of its methods of printing checks. **The Transform range of solutions enables you to manage all of your document-centered process needs. Use it to: Design and produce high quality business documents that present data accessed from a range of sources. Distribute documents through print, fax, or email in formats such as PDF, PDF/A, XML, HTML, and MHTML. Store, find, and retrieve documents within a secure web archive. Use OCR technology to capture documents and correspondence arriving in your organization and improve efficiency of the capture processes. Design workflows that support user interaction through Web interfaces to automate your document-centered business processes. ** Copied from Transform 5.3 release notes created by Bottomline Technologies August 2014.	No	HHSA Full Support
Traverse	Plots mapping coordin/ates & creates a map from the coordin/ates. Used by Assessor Mapping Dept	No	FG3 Coordinated Support
TreePlotter	TreePlotter is comprehensive web-browser based GIS software application for field data collection of tree and other green asset data management. Requires Chrome or Safari; Edge is not as fully supported but the app generally works in other browsers. There is no specific patching schedule, our devs regular evaluate and upgrade or patch servers, libraries and apps.	No	LUEG Coordinated Support
Trint - Multi- Language Transcription Service	Transcription service for D4's social media videos that transcribes in multiple languages. Allows accessibility of the videos for all constituents.	Yes	FG3 SaaS Support
Tririga	Tririga is a comprehensive solution that allows DGS to manage its activities across its business units. Specifically, the integrated capabilities include: Asset management (building equipment, keys, land, etc.) Work order management Preventive maintenance scheduling Reporting and tracking of capital and major maintenance projects Space planning and forecasting Service contract billing and chargeback to customers Management and monitoring of real estate leases Facility condition assessment Time tracking per work effort and integration with KRONOS	Yes	FG3 SaaS Support
Tririga Facility Center	Facilities space, lease, maintenance & consrtuction project management application. The Department of General Services (DGS) provides a wide range of services to other County Departments. DGS uses the IBM Tririga (formerly known as Tririga Facility Center) application in its support of these services, and hosts its Tririga environment with Gilbane i.management (Gilbane) in an ASP support model.	No	FG3 Coordinated Support
TTC Ad-Hoc Bill Printing	Mainframe on demand tax bill printing with HP printers and use consistent forms/formats between the bulk and ad-hoc tax bills for the various bill types on all tax rolls. This project will also allow those same tax bills to be printed in PDF format and placed in a shared folder for use by authorized TTC personnel.	No	FG3 Coordinated Support
TTC AEM Internet Site (SDTTC.COM)	TTC web site WWW.SDTTC.COM on the AEM platform (Adobe Experience Manager)	No	FG3 Full Support
TTC ApplicationXtender and WebXtender	Documentum ApplicationXtender Product Suite (File Access Manager, WebXtender (aka. AX .NET Web Access), and AppXtender).	No	FG3 Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
TTC Automated Lien Recording Application	TTC currently utilizes a workstation based process with dependencies on (3) MS-Access Databases to electronically submit Tax Lien documents to the SECURE Electronic Recording Delivery System (ERDS) Portal for recording of documents. Orange County has developed an Automated Lien Recording component to submit the Tax Lien documents using the SECURE API so that batch submittal process is automated (as opposed to single file drag and drop method that TTC previously utilized).	No	FG3 Full Support
TTC Bloomberg Gateway	Monitor stock market; track stock history; obtain news events critical to stock market; chart stocks; perform "what if" scenarios.	No	FG3 Coordinated Support
TTC Business Intelligence (TTCBI)	TTCBI is a Power BI reporting system used by the IPTS group. Reports were developed using Power BI Desktop and Power BI Report Builder.	No	FG3 Full Support
TTC CMS	Cloud-Based email subscription service for the Treasurer-Tax Collector to notify the public about important property tax information.	No	FG3 Coordinated Support
TTC CRS (Central Reporting System)	CRS is part of the custom-developed TTC WITS (PA2581) framework. Imports County of San Diego property tax payments from six payment systems: Cashiering, mail, CORTAC, eLockbox, web, and IVR phone payments. Imported via an applications scheduler and web-based user interface to collect, process, and reconcile property tax payments for transmission to the Mainframe. Exchanges data with an Oracle database, which stores data and performs back-end data processing and produces a number of reports. An end-of-day process creates a formatted file on another server for scheduled Mainframe processing. The output is a reconciled property tax bill and a number of reports.	No	FG3 Full Support
TTC Debt Management System	The County, through the TTC, has entered into agreements with school districts and community colleges in the county, to act as the paying agent and registrar for over 200 bond issuances. In its role as paying agent, the TTC pays the principal of, redemption premium, if any, and interest on each bond in accordance with the provisions of the bond resolutions under which the bonds are issued. Replace the current MS Access solution with SAP Sybase SQL anywhere client server solution.	No	FG3 Coordinated Support
TTC Electronic Relationship Management	TTC Electronic Relationship Management (eRM) application is a custom application built by Perspecta and RSM US LLC for the Treasurer-Tax Collector. The application resides on the CoSD Microsoft O365 Government Cloud and uses the Dynamics 365 application. The application will be a way for the TTC department to track tax payer activities across a number of use-cases.	No	FG3 Full Support
TTC EPS Express Manager	Transaction Database and report generation tool for IVR and Web Tax Payments.	No	FG3 Coordinated Support
TTC Interactive Web Response (IWR)	This is a 24/7 public facing website for constituents to view and pay their property tax bills online via E-Check or credit card. Payments are processed through a third-party vendor, Heartland Payment Systems (HPS). Post-payment data is returned and stored in the EPS database. IWR interfaces with the following PAIDs for tax collection: PA1308 - TTC Sonant IVR, ACD, and Phone Payment System, PA2438 - TTC WITS, and PA2601 - TTC EPS. Taxpayers can access the IWR website on any web-capable device (www.sdttc.com). CoSD TTC Financial staff must be authorized for access to the IWR environment to manage the maintenance web page. Sonant and Perspecta technical staff have access to the environment to support the application using County AD accounts.	No	FG3 Full Support
TTC iPayment Cashiering	Browser based property tax cashiering application.	No	FG3 Coordinated Support
TTC J.P. Morgan Chase Banking	Banking for County of San Diego	No	FG3 Coordinated Support
TTC Mobile Home Tax Clearance Database	TTC Mobile Home Tax Clearance Database is an MS Access 2016 database located on a NAS share that the users must be granted access to. It receives a once-per-year data transfer that is manually imported into the MS Access database. Perspecta is responsible for managing the application. The MS Access application runs on Citrix. Users receive a desktop icon as part of the Citrix client install package.	No	FG3 Coordinated Support
TTC Phone Payment System	Interactive Voice Response (IVR) system for the purpose of paying property taxes over the phone via credit card	No	FG3 Coordinated Support
TTC SeeTrans	Application to query historical tax payment transactions	No	FG3 Full Support
TTC Sharepoint iTTC	TTC requires a SharePoint Site Collection instance in the collaboration space that is supported by ES, as it will house TTC's official intranet for interdepartment and intradepartment view only. In the future, TTC will submit requests via VLRs to create forms and workflows in this site collection instance. This SharePoint site will reside in the GCC and use SharePoint Online	No	FG3 Full Support
TTC Sonant IVR, ACD and Phone Payment System	Interactive Voice Response (IVR) system, created by Sonant Corporation, allows taxpayers to use a telephone to pay their property tax payment, have a duplicate tax bill mailed to them, or transfer to another system called Automated Call Distribution (ACD) system which permits them to make property tax payment inquiries. The IVR system accesses the Master Tax File on the mainframe and the Web Integrated Tax System (WITS) for payment status to obtain property tax information.	No	FG3 Coordinated Support
TTC Sympro	Sympro is Treasury Management System. The software is access by securing a VPN Connection and RDP to a Vendor hosted server. Sympro has replaced Sungard.	No	FG3 Coordinated Support
TTC Tax Sale Database	Control, reporting of property eligible for Public Tax Sale; includes a Point-Of-Sale Module.	No	FG3 Full Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
TTC TRCC Cortac (Mainframe)	Generate electronic media for tax agencies	No	FG3 Full Support
TTC TRDS Defaulted Secured Data Mgmt (Mainframe)	Tax Collector system for managing secured tax billing and collections for accounts that are in default	No	FG3 Full Support
TTC TRRT Unsecured Tax Refund Mgmt System (Mainframe)	Tax Collector system for managing refund actions for Unsecured property tax accounts	No	FG3 Full Support
TTC TRST Tax Collector Secured Tax Collect (Mainframe)	Tax Collector system for collecting and managing Secured property tax bill amount for the current year	No	FG3 Full Support
TTC TRTC Carryover (Mainframe)	Secured Property Tax - Carry Over Roll	No	FG3 Full Support
TTC TRTH Secured Tax History Info System (Mainframe)	Tax Collector system used to display 5 most current years of Secured Tax billing and collection history data by parcel	No	FG3 Full Support
TTC TRUS Unsecured Property Tax System (Mainframe)	Maintains unsecured property tax master files. Posts Wits tax payments, computes penalties, generates reports, produces bulk tax bills and on-demand tax bills for remote printers. Provides interfaces to Wits and IVR payment packages and Trustref refunds.	No	FG3 Full Support
TTC Trustref (TTC Financial Apps)	Financial Reporting System for taxpayer refunds.	No	FG3 Full Support
TTC WARP (Wire Access Request Portal)	External entities wire request system. Used by school districts and other external entities for whom the County manages funds collected for those entities via taxes. This is just a "workflow" application where external entities request a wire transfer of tax funds from their County managed account to their bank. The actual wire transfer of those funds is made via a different application.	No	FG3 Full Support
TTC Wausau ImageRPS	Image Based Remittance Processing System	No	FG3 Coordinated Support
TTC Web Payment System	Heartland Payment System (HPS) is an off-site credit card and echeck payment system utilized by TTC for their Web tax payment systems. HPS has developed the Frontend Web-site and the back-end CC and eCheck processing for the web site. HPS is a subcontractor to Perspecta	No	FG3 Full Support
TTC WITS (Web Integrated Tax System)	This Web Integrated Tax System (WITS), PA2438, is a series of custom web services and methods that interface with payment systems provided by CoSD vendors. The WITS application interfaces with the CoSD Mainframe and contains business rules that send the proper tax payment information to the various tax payment system.	No	FG3 Full Support
Twitter	Social Media Site	Yes	FG3 SaaS Support
Unique Management Chat Service	Unique Management Services will provide chat support to Library customers through the website www.sdcl.org. This support would address any questions customers may choose to get a response to through the chat service. This would offload a large portion of this support function from Library staff, thereby allowing them to offer more programs and to provide personal service to customers at the Branch.	Yes	LUEG SaaS Support
Uptime Robot	It monitors your websites every 5 minutes and alerts you if your sites are down.It asks for your websites headers and gets status codes like "200-ok", "404-not found", etc. every 5 minutes (or more depending on the monitor's settings),If the status code doesn't indicate a problem, we are goodIf the status code is~400+ and 500+, then the site is not loadingIn order to make sure the site is down, Uptime Robot makes several more checks in the next 30 seconds,If the site is still down, it sends an alert.	Yes	PSG SaaS Support
uQR.me	The vendor provides QR codes which redirect traffic to County public AEM pages. The vendor provides traffic analytics through Google Analytics for Businesses, and all the information is stored by Google and anonymized.	Yes	LUEG SaaS Support
US Bank	TTC Treasury Division will use software to manage, track, and verify bond payments made by a bank paying agent for the 42 school districts and 5 community college General Obligation Bonds for the County of San Diego.	Yes	FG3 SaaS Support
Utility Manager Pro	Track and report on utility usage costs - specifically for SDG&E invoices received by the County.MS Access Database accessed by client software on users desktop computers - Desktop shortcut should be: “C:\Program Files (x86)\LPB Energy Management\UtilityManager\UM40.EXE” "U:\utilitymanager\UM40.MDB" ; Drive Shared Mapping: U = \\USTLGPCSD0002\UtilityManager	No	FG3 Coordinated Support
Vector Mobile Inspection	CityGov Application: Vector Mobile App gives field technicians an easy and effective way to access and enter Accela data while in the field.	No	LUEG Coordinated Support
VectorSolutions	The Vector Learning Management System (LMS) is a Training Solution built with unique features and functionality to fit the training needs of critical industries. It provides one place for all of your training needs - from assigning, tracking and reporting on course completions, to tracking license and credential requirements, to identifying employee skill gaps. The Vector LMS makes it easier to build a culture of training, safety, and compliance.	Yes	LUEG SaaS Support
Veriform	VeriForm is a checklist management system that helps ensure that staff are following standardized protocols essential to meeting quality objectives and improving care. For example, checklists can help make sure that medications are properly stored in areas outside of the cleanroom.	Yes	HHSA SaaS Support
Verizon Wireless Email to Text for Pollworkers	Verizon Wireless provided services for ROV staff to send mass email reminders to text messaging to over 8000 Pollworkers. This application is accessed through the Verizon Wireless portal where the ROV staff can send text messages to pollworker cell phones.	Yes	FG3 SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
Vet Pro Web	Veteran Case Management software application, developing & tracking claims and awards for veterans, mandated by CA Dept of Veterans Affairs	Yes	HHSA SaaS Support
Video Management System	A single application to access all HHSA security cameras feeds from one interface. The functionality includes: Administration, view multi-display, personalized dashboard with alarm widgets, track key indicators in one center location, video events and system health in real time, and the ability to provide instant access to federated entities such as CoSD Sheriff. Support is a combination of Perspecta and Vendor.	No	HHSA Coordinated Support
Viking Data Entry System	Viking Data Entry (VDE) is used by ARCC to capture forms data elements from various property assessments, appraisals, change in ownerships, claims, and other documents. The captured data elements are validate and compiled into custom formatted batches for high speed ingestion into the mainframe for Real Property updates.	No	FG3 Full Support
Vimeo	Human Resources Talen Development Division produces video segments that are incorporated into our E-Learning trainings. The video's need to be uploaded to a platform that can handle the bandwidth needed to stream an HD video to multiple users. YouTube is a solution we have used in the past, but due to the ads, the inability to replace/update a video with the same url, and the limited privacy functions we feel VIMEO.com is a more robust solution.	Yes	FG3 SaaS Support
Vimeo	Founded in 2004, Vimeo is a web-based video hosting tool. Vimeo allows you to create, share, and discover videos online and worldwide. Vimeo has redundant data centers to help with having high-speed playback and redundancy for backup.	Yes	PSG SaaS Support
Visme	Visme will be used as a tool to help communicate project management timelines, milestones, and relevant project information (via one-pagers, fact sheets, and process/logic flow models) to internal team members (project staff, ops staff and BHS executives) and other CoSD HHSA staff through engaging and professional static digital content.Visme is different from already available solutions (Visio, Microsoft Publisher, PowerPoint, etc.) in the sense that it is significantly more user friendly, and offers a large portfolio of standard layouts and Templates. The large volume of projects that the BHS PMO manages requires the use of a more efficient and user-friendly solution. The application is hosted on Amazon Web Services and their data center is located in the US region (northern VA). Visme owns their own servers at AWS. Data is encrypted at rest and are 100% secure.	Yes	HHSA SaaS Support
Vital Records Information System	VRIS is a web user interface for coding death and fetal certificates. This is the main functionality of the utility. Data captured and reviewed from this process then gets stored to the Vitals database (used to be called IDCMS) and also gets exported to AppXtender. Application servers are using F5 load balancing.	No	HHSA Full Support
VitalChek	VitalChek Network Inc. is a secure web based solution for credit card transaction processing. VitalChek allows HHSA program to provide faster service to the customers due to real time receipts of credit card payment.	Yes	PSG SaaS Support
Volunteer Tracking System AIS	Volunteer management software that is used by the Ombudsman Program	No	HHSA Coordinated Support
Voter Roster Capture	The San Diego Registrar of Voters (SDROV) will implement a capture solution to scan pre-printed Rosters of Voters and automatically recognize and extract the Voter IDs of voters that cast a ballot. Handwritten rosters associated with provisional ballots would also be scanned, but no Voter IDs would be extracted.A key project goal is to be able to capture approximately 250,000 pages of rosters and upload the extracted Voter IDs within several business days. Accurate Voter ID recognition is mandatory.1. Phase 1 will include form design, scan/capture, and export components of post-processed data for saving images as flat files on SAN/NAS storage as well as comma-separated value file for importing to EMS.	No	FG3 Full Support
Vyond (was GoAnimate)	Vyond is a monthly subscription that gives our multimedia designers access to a library of animated characters and backdrops and then create animated videos for use in County online trainings and videos.	Yes	FG3 SaaS Support
Wasp AssetCloud	App sescription from provider website, https://www.waspbarcode.com/asset-tracking: "Wasp is the only asset tracking solution provider that offers all the necessary software, hardware, and asset tags you need to implement an asset management system. This makes AssetCloud not only the most feature-rich asset tracking software in the industry, but also makes it the most complete solution available from one provider." "Easy-to-Use Asset Tracking Software.Automate your organization's fixed asset tracking for improved check-in/check-out processes, faster auditing, and error-free reporting."	Yes	PSG SaaS Support
Weather Monitoring and Flood Warning System	Hydstra is a software for managing large amounts of time-series data in the hydro power, water resources and wastewater industries. Hydstra offers a complete solution to environmental data management conducting: Data Acquisition Data Management Data Analysis Modelling and Simulation Automated Task Scheduling	No	LUEG Full Support
Web Application for Legacy Payroll Data and Reports	Web front end for reports for Legacy Payroll data migration for the Human Resources Payroll System and the Online Payroll History.	No	FG3 Full Support
Web Confidential Morbidity Report (WebCMR)	A web base solution for tracking and reporting disease incidents and outbreaks using a comprehensive suite of case management tools.	Yes	HHSA SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Application	Description	Cloud App?	Bundle
WebEOC	WebEOC provides crisis coordination for the San Diego Operational Area. It is used to share information during disasters or planned events that require coordination between emergency responders. This does not provide any direct information to the public. This is for Emergency responders and decision makers only.	Yes	PSG SaaS Support
WebTrak (ANOMS)	WebTrak (ANOMS) is a system provided to the citizens which allows them to access a website to view flight information around McClellan Palomar Airport. Citizens can identify an aircraft and submit noise complaints online. Airport staff then use a back office system (ANOMS) to review flight logs to determine if a violation occurred.	Yes	LUEG SaaS Support
Weebly	Website design, hosting, storage, and support for Aging & Independence Services websites.	Yes	HHSA SaaS Support
Wellness Incentive	SharePoint site to automate the processing of the Wellness Incentive program by allowing the submission of the necessary documentation in order to be eligible for the incentive payout. Participants currently submit two documents via email for processing. If it is determined that the documents are complete, certain information (Employee Name, ID, etc) is sent to Central Payroll for the payout. It is vital that duplicates are not submitted. This site handles the submission and approval. Once approved, the process to send data to central payroll is not part of this site.	No	FG3 Full Support
Western Limited, Inc - Investigative Services	Western LimitedThe vendor will receive a request that includes personal identifiable information and medical information; this information will be entered into their system in order to perform the services requested and then provide a report (that contains such information), which may include video.	Yes	FG3 SaaS Support
Westlaw Form Builder	Used to facilitate legal document/form assembly.	Yes	FG3 SaaS Support
When I Work	Workforce scheduling SaaS service that will be used by county staff to schedule nurses and healthcare volunteers working in alternate care centers in support of COVID-19 response. Nurses and volunteers will access the service to view schedules and work assignments.	Yes	HHSA SaaS Support
When2Work	When2Work is a web based work shift scheduling app for 200+ election workers and 100+ MBDO locations.	Yes	FG3 SaaS Support
WITS	ADS system that tracks data for CALOMS WITS is a centrally hosted administrator supported data processing system designed for reuse by State substance abuse & mental health services agencies & SAMHSA grantee programs . It supports realtime data processing starting with data collection at treatment clinics This application is hosted by the vendor group SAMHSA (Substance Abuse & Mental Health Services Administration) . SAMHSA manages the general administration of the WITS program through it subsidiaries . For more details about SAMHSA access the website : http://www.samhsa.gov/about Contact Info: Richard Thoreson Email:Rthoreso@SAMHSA.gov Phone: (301) 443- 5325	No	HHSA Coordinated Support
Wonderware SCADA IAAS Services	The Wonderware SaaS System is a basic station control and data acquisition (SCADA) system which will monitor and manage various wastewater facilities across San Diego county.	Yes	LUEG SaaS Support
Workflow Manager for Revenue and Recovery Remittance System	WebServer IIS front end	No	FG3 Full Support
Workschedule.net	This is a staff work scheduling system for our facilities that operate 24/7.	Yes	PSG SaaS Support
YouTube	Social Media Video Site	Yes	FG3 SaaS Support
Zoll Case Review Software	Quickly transmit essential clinical data, includingCPR quality, ECG, and EtCO2, directly from anX Series® Advanced monitor/defibrillator orZOLL AED 3® BLS defibrillator. The pushof a button ensures that key metrics aredelivered to QA/QI personnel no cards or cables are required	Yes	PSG SaaS Support
Zoom Business	Zoom is a video communications company that affords its users video conferencing remotely using cloud-based computing. It is a Software as a Service (SaaS) that provides you with an easy and stress-free platform to hold online meetings, mobile collaboration as well as video conferencing.	Yes	HHSA SaaS Support
Zoom Pro with Webinar/Event Addon	OERJ staff will use Zoom Pro with Webinar/Events add-on to provide virtual meetings with collaboration to the public and constituents with the option for interpretation.	Yes	FG3 SaaS Support

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - County Bundle

Bundle	Annual Price Point
Full Support	$7,239,151.69
Coordinated Support	$2,355,531.01
SaaS Support	$109,004.57

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Group Bundle

OPTION NOT EXERCISED

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Portfolio Applications

Exhibit 16.1-5 Firm Fixed Price for Applications Maintenance & Operations - Low Org Bundle

OPTION NOT EXERCISED

Exhibit 16.1-5b – Firm Fixed Price for Applications Maintenance and Operations

Table of Contents

1. Overview 3

2. Firm Fixed Price Model....3

2.1. Overview 3

2.2. Periodical Review by Applications Review Board (ARB)....3

2.3. New Portfolio Applications....4

2.4. Retired Portfolio Applications....4

3. Annual Fee....4

3.1. Applications M&O Fee Options....4

3.2. Applications M&O Fee Option Selected....5

3.3. Annual Reduction in Cost 5

1. OVERVIEW

This Exhibit describes the methodology for billing with respect to Applications Maintenance and Operations (M&O).

2. FIRM FIXED PRICE MODEL

2.1. Overview

Contractor shall provide a Firm Fixed Price (FFP) option for Applications M&O. The Applications M&O FFP activities shall be maintained in the Standards and Procedures and shall be supported by the administration and maintenance of the Break/Fix environment (included in the Development & Test Services Resource Unit) as per tables below.

Costs	Services					
	Applications Development Service	Applications M&O Service	Production Infrastructure (servers and storage)	All Storage (not Production)	Physical Server/Virtual Servers (not Production)	Backups
Applications M&O FFP	Not included	Included	Not included	Not Included	Not Included	Not Included
Development / Test FFP	Not included	Not included	Not included	Included for Development / Test and Break/Fix Usage	Included for Development / Test and Break/Fix Usage	Included for Development / Test and Break/Fix Usage

Costs	Managed Private Cloud			
	Development / Test Physical HOSTS For Virtual Environment	Development / Test Virtual Environment	Break/Fix Physical HOSTS For Virtual Environment	Break/Fix Virtual Environment
Applications M&O FFP	Not included	Not included	Not included	Not included
Development / Test FFP	Included	Included	Included	Included

The Applications M&O shall consist of three categories of support: Full, Coordinate, and SaaS. Applications will be placed in the applicable support category per the Standard and Procedures.

2.2. Periodical Review by Applications Review Board (ARB)

An ARB shall be established to perform a collaborative evaluation of the applications that have been enhanced, added to or retired from the FFP Application List and determine whether the Applications M&O Resource Unit Fee warrants adjustment. The ARB shall meet quarterly and upon County request or

in the event Contractor identifies a material change to the FFP Application List as further detailed in the Standards and Procedures. A material change is defined as additions or deletions of applications from the FFP Application List that affect the M&O support and/or server environment, and that meet any of the following criteria:

1. Affects fifty (50) or more End-Users.
2. Requires addition or deletion of five (5) or more servers to/from Development / Test environment.

2.3. New Portfolio Applications

For incremental changes to the FFP Applications List - Full and Coordinated Support categories, Contractor shall evaluate the support, operations, and maintenance requirements for such change and determine whether those requirements present a change in the workload and then propose the appropriate FFP Fee adjustments to the ARB, as per the process set forth in the Standard and Procedure Manual.

In the event that there is a net add of 100 applications to the FFP Applications List - SaaS Support category in the Contract Year, Contractor shall evaluate adjustment to the FFP and if applicable, propose the appropriate FFP Fee adjustment to the ARB. The net add threshold will be reviewed at the end of the Contract Year and adjusted upon mutual agreement between Parties.

2.4. Retired Portfolio Applications

For retired applications in the FFP Applications List - Full and Coordinated Support categories, Contractor shall evaluate the support, operations, and maintenance requirements for the incremental change and determine whether those requirements present a change in the workload and then propose the appropriate FFP Fee adjustments to the ARB, as per the process set forth in the Standard and Procedure Manual. Retired applications are defined as applications no longer being used by the County and have been requested by County to be removed from the portfolio.

3. ANNUAL FEE

3.1. Applications M&O Fee Options

Contractor shall provide the following Applications M&O FFP options: Low Org, Group and County. The FFP options will breakdown the annual fee by support category: Full, Coordinate, and SaaS. County may select one of the options at the onset of the Agreement and such option will be in place through end

of Contract Year (CY) 2. Effective CY3, County may select a different FFP option or move to a time and materials (T&M) pricing model with a 60-day prior notice to Contractor. Combining any of the FFP options with T&M is not allowed.

In the event that the County selects a different FFP option in CY3 or any subsequent CY, Contractor shall at that time provide County with updated pricing for all FFP options for review. The updated pricing shall breakout the FFP options at the support category level. In the event that the County selects the T&M pricing model in CY3 or any subsequent CY, the principles and process set forth in the Schedule 4.3-1 Contractor's Solution, *Alternate Time & Materials model to provide Applications Maintenance and Operations services*, shall be applied.

Contractor shall prorate the FFP over twelve (12) months and charge the County a fixed monthly Resource Unit (RU) Fee for Applications M&O accordingly. The FFP is subject adjustment based on ARB decisions, and annual reduction in fees starting CY3.

3.2. Applications M&O Fee Option Selected

The table below provides the Applications M&O Fee option selected by the County for Contract Year.

Contract Year	Applications M&O FFP Option
1	County Level
2	County Level
3	County Level
4	County Level
5	County Level
6	County Level
7	County Level
8	County Level

3.3. Annual Reduction in Cost

Contractor shall reduce the annual cost of Applications M&O FFP from previous year as per the table below. Contractor shall base the reduction on the overall Applications M&O FFP at the end of the fiscal year. Optional Year Percentage Reduction will be negotiated based on experience during the Base Period.

Contract Year	Percentage Reduction
2	0%
3	2%
4	2%
5	2%
6	2%

Contract Year	Percentage Reduction
7	2%

END OF EXHIBIT

Exhibit 16.1-6 – Resource Unit Price Summary Option Term

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Contract and Acquisition Management Services	****Schedule 4.3 - Section 2.3	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 222,400.64	$ 2,668,807.71	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Integrated Asset Management Services	Schedule 4.3 - Section 2.4	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 118,445.02	$ 1,421,340.21	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Billing Management Services	Schedule 4.3 - Section 2.5	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 43,985.05	$ 527,820.62	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Security Management Services	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 252,784.50	$ 3,033,414.03	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Malware Protection	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 5,270.06	$ 63,240.72	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Secure Internet Access	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 28,211.10	$ 338,533.20	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Enterprise Application Access	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 78,203.57	$ 938,442.84	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Multi-Factor Authentication Service	Schedule 4.3 - Section 2.6	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 43,883.82	$ 526,605.84	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Delivery Management Services	Schedule 4.3 - Section 2.7	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 207,383.46	$ 2,488,601.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Project Management Services	Schedule 4.3 - Section 2.9	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 140,665.48	$ 1,687,985.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Integration and Testing Services	Schedule 4.3 - Section 2.10	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 38,164.21	$ 457,970.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Incident Management Services	Schedule 4.3 - Section 2.11	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 3,482.29	$ 41,787.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Problem Management Services	Schedule 4.3 - Section 2.12	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 3,482.29	$ 41,787.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Change Management Services	Schedule 4.3 - Section 2.13	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 9,776.47	$ 117,317.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Release Management Services	Schedule 4.3 - Section 2.14	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 11,001.46	$ 132,017.56	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Configuration Management Services	Schedule 4.3 - Section 2.15	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 18,978.04	$ 227,736.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Capacity Planning and Performance Management Services	Schedule 4.3 - Section 2.16	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 18,372.67	$ 220,472.04	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Disaster Recovery Management Services	Schedule 4.3 - Section 2.17	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 194,230.46	$ 2,330,765.53	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Identity Access Management Services	Schedule 4.3 - Section 2.18	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 137,432.70	$ 1,649,192.45	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Reporting Management Services	Schedule 4.3 - Section 2.19	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 77,693.51	$ 932,322.11	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Domain Name Management Services	Schedule 4.3 - Section 2.20	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 1,599.85	$ 19,198.24	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Business Analyst Services	Schedule 4.3 - Section 2.21	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 83,261.44	$ 999,137.31	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Chief Technical Architect Services	Schedule 4.3 - Section 2.22	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 19,097.64	$ 229,171.65	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Enterprise Applications Architect Services	Schedule 4.3 - Section 2.23	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 19,097.64	$ 229,171.65	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Innovation Management Services	Schedule 4.3 - Section 2.24	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 21,073.13	$ 252,877.59	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Desk Services	Schedule 4.3 - Section 3	Service Desk Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 184,350.93	$ 2,212,211.18	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Duo Hardware Token MFA	Schedule 4.3 - Section 4.5.2	End User Services	Account	Fixed Monthly Fee Per Unit		Specific	10	$ 5.28	$ 52.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Electronic Signature Service	Schedule 4.3 - Section 4.5.2	End User Services	Transaction	Fixed Fee Per Unit		Cumulative	25,000	$ 1.01	$ 25,250.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Desktop - 3D Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	396	$ 254.53	$ 100,794.55	$ 279.58	$ 265.76	$ 248.40	$ 243.11	$ 238.66	$ 234.29	3

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Desktop - Advanced Engineering Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	**	$ 195.52	$ -	$ 214.75	$ 204.14	$ 190.80	$ 186.74	$ 183.32	$ 179.97	4
Desktop - Advanced Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	**	$ 87.52	$ -	$ 96.13	$ 91.38	$ 85.41	$ 83.59	$ 82.06	$ 80.56	4
Desktop - Engineering Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3,228	$ 103.35	$ 333,610.70	$ 113.52	$ 107.91	$ 100.86	$ 98.71	$ 96.90	$ 95.13	4
Desktop - Gold Engineering Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	44	$ 275.02	$ 12,100.86	$ 302.08	$ 287.15	$ 268.39	$ 262.67	$ 257.87	$ 253.15	4
Desktop - Mini Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	250	$ 60.41	$ 15,103.20	$ 66.36	$ 63.08	$ 58.96	$ 57.70	$ 56.65	$ 55.61	4
Desktop - Small Form Factor with Optical Drive	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	250	$ 60.41	$ 15,103.20	$ 66.36	$ 63.08	$ 58.96	$ 57.70	$ 56.65	$ 55.61	4
Desktop - Standard Workstation	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	112,776	$ 60.41	$ 6,813,113.93	$ 66.36	$ 63.08	$ 58.96	$ 57.70	$ 56.65	$ 55.61	4
Desktop - Scanner	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	528	$ 139.09	$ 73,439.52	$ 153.00	$ 144.65	$ 136.31	$ 133.53	$ 130.74	$ 127.96	4
Laptop - Engineering	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	900	$ 156.01	$ 140,408.42	$ 171.36	$ 162.89	$ 152.25	$ 149.01	$ 146.28	$ 143.60	3
Laptop - Ruggedized	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	636	$ 175.15	$ 111,393.43	$ 192.38	$ 182.87	$ 170.93	$ 167.29	$ 164.22	$ 161.22	3
Laptop - Standard	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	37,212	$ 80.49	$ 2,995,249.70	$ 88.41	$ 84.04	$ 78.55	$ 76.88	$ 75.47	$ 74.09	3
Laptop - Standard LTE	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	100	$ 100.90	$ 10,090.00	$ 110.82	$ 105.34	$ 98.46	$ 96.36	$ 94.60	$ 92.87	3
Laptop - Ultra Portable	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	10,392	$ 87.29	$ 907,144.60	$ 95.88	$ 91.14	$ 85.19	$ 83.37	$ 81.85	$ 80.35	3
Laptop - Ultra Portable 2in1	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	372	$ 99.03	$ 36,838.86	$ 108.77	$ 103.40	$ 96.64	$ 94.58	$ 92.85	$ 91.15	3
Tablet - Convertible	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3,420	$ 88.61	$ 303,058.70	$ 97.33	$ 92.52	$ 86.48	$ 84.64	$ 83.09	$ 81.57	3
Tablet - Ruggedized	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	360	$ 195.14	$ 70,251.08	$ 214.34	$ 203.75	$ 190.44	$ 186.38	$ 182.97	$ 179.62	3
Tablet - Surface Pro	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	3480	$ 99.43	$ 346,031.03	$ 109.22	$ 103.82	$ 97.04	$ 94.97	$ 93.23	$ 91.53	3
Tablet - Surface Pro LTE	Schedule 4.3 - Section 4.5.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	100	$ 127.64	$ 12,764.00	$ 140.20	$ 133.26	$ 124.56	$ 121.91	$ 119.68	$ 117.49	3
Early Refresh - Desktop	Schedule 4.3 - Section 4.5.4	End User Services	Month	Fixed Fee Per Unit		Specific	13	$ 34.00	$ 442.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Early Refresh - Mobile PC	Schedule 4.3 - Section 4.5.4	End User Services	Month	Fixed Fee Per Unit		Specific	1	$ 47.00	$ 47.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
County Retained Device	Schedule 4.3 - Section 4.7.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	48	$ 95.87	$ 4,601.94	$ 105.31	$ 100.10	$ 93.56	$ 91.57	$ 89.89	$ 88.25	3
Desktop - DCSS	Schedule 4.3 - Section 4.7.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	6,432	$ 33.69	$ 216,689.26	$ 37.00	$ 35.17	$ 32.88	$ 32.18	$ 31.59	$ 31.01	n/a
Laptop - DCSS	Schedule 4.3 - Section 4.7.3	End User Services	Device	Fixed Monthly Fee Per Unit	B1	Specific	180	$ 41.21	$ 7,417.49	$ 45.26	$ 43.03	$ 40.22	$ 39.36	$ 38.64	$ 37.93	n/a
Printer - Color Network Workgroup - Large Format (CNWP-LF)	Schedule 4.3 - Section 4.11.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	528	$ 154.16	$ 81,398.72	$ 169.33	$ 160.96	$ 150.45	$ 147.24	$ 144.55	$ 141.90	4
Printer - Color Network Workgroup - Standard Format (CNWP)	Schedule 4.3 - Section 4.11.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	2,328	$ 62.84	$ 146,299.33	$ 69.03	$ 65.61	$ 61.33	$ 60.02	$ 58.92	$ 57.85	4
Printer - Monochrome Network Workgroup - Standard Format (MNWP)	Schedule 4.3 - Section 4.11.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	8,964	$ 56.25	$ 504,267.76	$ 61.79	$ 58.74	$ 54.90	$ 53.73	$ 52.75	$ 51.78	4
Printer - Monochrome Network Workgroup - Large Format (MNWP-LF)	Schedule 4.3 - Section 4.11.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	264	$ 90.61	$ 23,921.47	$ 99.53	$ 94.61	$ 88.43	$ 86.54	$ 84.96	$ 83.41	4
Printer - Monochrome Network High Volume - Large Format (MNWP-LF-H)	Schedule 4.3 - Section 4.11.3	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	312	$ 147.76	$ 46,101.12	$ 161.05	$ 154.26	$ 145.06	$ 142.40	$ 139.80	$ 137.24	4
Electronic File Sharing Services	Schedule 4.3 - Section 4.12	End User Services	User	Fixed Monthly Fee Per Unit		Specific	1,212	$81.25 (101-250)	$ 98,475.00	$56.55 (251-500)	$47.83 (501-1000)	$42.18 (1001+)	n/a	n/a	n/a	n/a

Exhibit 16.1-6 Resource Unit Price Summary Option Term																
Resource Unit (RU)	***Reference**	**Framework**	**Unit of Measure**	**Pricing Method**	**Bundle**	**Measurement Method**	**Baseline Volumes (per Contract Year)**	**RU Fee (90-110% band)**	**Baseline Annual Fee**	**RU Fee (70% to 80% band)**	**RU Fee (80% to 90% band)**	**RU Fee (110% to 120% band)**	**RU Fee (120% to 130% band)**	**RU Fee (130% to 150% band)**	**RU Fee (150% to 200% band)**	**Depreciation Period (in Years)**
A/V Conference Room - Large	Schedule 4.3 - Section 4.13	End User Services	Install	Fixed Fee Per Unit		Cumulative	1	$ 64,563.91	$ 64,563.91	n/a	n/a	n/a	n/a	n/a	n/a	n/a
A/V Conference Room - Medium	Schedule 4.3 - Section 4.13	End User Services	Install	Fixed Fee Per Unit		Cumulative	1	$ 34,671.93	$ 34,671.93	n/a	n/a	n/a	n/a	n/a	n/a	n/a
A/V Conference Room - Small	Schedule 4.3 - Section 4.13	End User Services	Install	Fixed Fee Per Unit		Cumulative	1	25,005	$ 25,004.76	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Digital Signage Services	Schedule 4.3 - Section 4.14	End User Services	Subscription	Fixed Monthly Fee Per Unit		Specific	2400	$ 73.84	$ 177,215.04	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Survey Solution Support Services	Schedule 4.3 - Section 4.16	End User Services	Subscription	Fixed Monthly Fee Per Unit		Specific	360	$ 48.94	$ 17,618.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Network Access - Static Wired	Schedule 4.3 - Section 5.5	Network Services	Device	Fixed Monthly Fee Per Unit	B2	Specific	27708	$ 59.74	$ 1,655,161.14	$ 68.39	$ 63.92	$ 58.54	$ 57.37	$ 56.22	$ 55.10	n/a
Network Access - Static Wired (Library)	Schedule 4.3 - Section 5.5	Network Services	Device	Fixed Monthly Fee Per Unit	B2	Specific	120	$ 51.26	$ 6,151.20	$ 58.69	$ 54.84	$ 50.23	$ 49.23	$ 48.25	$ 47.28	4/5
Uninterrupted Power Supply Support Services	Schedule 4.3 - Section 5.5	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12	$ 115.50	$ 1,386.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
GSMS Short Code Setup	Schedule 4.3 - Section 5.6	Network Services	Event	Fixed Fee Per Unit		Cumulative	1	$ 3,885.00	$ 3,885.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
GSMS Short Code Support	Schedule 4.3 - Section 5.6	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 1,507.63	$ 18,091.56	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Portal - External Users	Schedule 4.3 - Section 5.6	Network Services	User	Fixed Monthly Fee Per Unit		Specific	200	$ 8.00	$ 1,600.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Portal - Portfolio Application	Schedule 4.3 - Section 5.6	Network Services	Application	Fixed Monthly Fee Per Unit		Specific	0	$ 210.90	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
GSMS Messages	Schedule 4.3 - Section 5.6	Network Services	Message	Fixed Fee Per Unit		Cumulative	1,680,000	$ 0.028	$ 47,040.00	0 - 10,000 Messages $0.00	10,000 - 100,000 Messages $0.033	100,001 - 500,000 Messages $0.028	500,001 + Messages $0.023	n/a	n/a	n/a
Virtual Private Network Access - Level 1	Schedule 4.3 - Section 5.6	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	0	$ 9.880000	$ -	$ 11.26	$ 10.57	$ 9.68	$ 9.48	$ 9.28	$ 9.09	4
Virtual Private Network Access - Level 2	Schedule 4.3 - Section 5.6	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	20,952	$ 11.455500	$ 240,015.64	$ 13.12	$ 12.26	$ 11.23	$ 11.00	$ 10.78	$ 10.57	n/a
Calls: Casual Use	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	6,167,520	$ 0.017359	$ 107,060.71	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Conference Bridge	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	53,415,060	$ 0.001337	$ 71,438.43	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Directory Assistance	Schedule 4.3 - Section 5.7	Network Services	Call	Fixed Fee Per Unit		Cumulative	233	$ 0.517658	$ 120.61	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: International	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	1,535,088	$ 0.002329	$ 3,575.52	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Local	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	762,100,578	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Toll	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	194,183,047	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Long Distance (CA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	112,254,258	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Off-Net Long Distance (USA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	78,582,984	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: On-Net	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	0	$ -	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Toll Free 800 Service (CA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	91,282,130	$ 0.000334	$ 30,451.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Toll Free 800 Service (San Diego & Imperial)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	1,235,112,040	$ 0.00	$ 412,079.10	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Calls: Toll Free 800 Service (USA)	Schedule 4.3 - Section 5.7	Network Services	Seconds	Fixed Monthly Fee Per Unit		Cumulative	127,834,956	$ 0.00	$ 42,644.08	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Pay Phones	Schedule 4.3 - Section 5.7	Network Services	Phone	Fixed Monthly Fee Per Unit		Specific	36	$ 91.11	$ 3,279.79	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Phone - Microsoft (MS) Teams Phone Advanced Features	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	36,000	$ 17.690	$ 636,840.00	n/a	n/a	n/a	n/a	n/a	n/a	$ 5.00

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Voice-Avaya Legacy Support	Schedule 4.3 - Section 5.7.3	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 437,522.40	$ 5,250,268.80	n/a	n/a	n/a	n/a	n/a	n/a	5
IP Conference Phone	Schedule 4.3 - Section 5.7.3	Network Services	Phone	Fixed Monthly Fee Per Unit		Specific	299	$ 62.70	$ 18,747.30	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Analog Line	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	29,088	$ 50.74	$ 1,475,976.92	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Single-Line	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	137,400	$ 23.98	$ 3,294,852.00	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Multi-Line	Schedule 4.3 - Section 5.7.3	Network Services	Active Line	Fixed Monthly Fee Per Unit		Specific	152,568	$ 26.30	$ 4,012,538.40	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Mail	Schedule 4.3 - Section 5.7.3	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	159,060	$ 3.89	$ 618,573.61	n/a	n/a	n/a	n/a	n/a	n/a	5
Voice Mail to Email Services	Schedule 4.3 - Section 5.7.3	Network Services	Active Account	Fixed Monthly Fee Per Unit		Specific	448	$ 1.90	$ 850.55	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Phone – Microsoft (MS) Teams Phone Advanced Features	Schedule 4.3 Section 5.7.3	Network Services	Call Flow	Fixed Monthly Fee Per Unit		Cumulative	240	$ 32.56	$ 7,814.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Cloud Access Security Broker	Schedule 4.3 - Section 5.8	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 15,450.12	$ 185,401.44	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Town Hall Services	Schedule 4.3 - Section 5.9	Network Services	Event	Fixed Fee Per Unit		Cumulative	0	$ 76,730.20	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Video Conferencing Services - Personal	Schedule 4.3 - Section 5.9	Network Services	System	Fixed Monthly Fee Per Unit		Specific	780	$ 331.49	$ 258,558.30	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Video Conferencing Services - Room System	Schedule 4.3 - Section 5.9	Network Services	System	Fixed Monthly Fee Per Unit		Specific	48	$ 955.44	$ 45,860.99	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Zoom Video Conferencing Support Services	Schedule 4.3 - Section 5.9	Network Services	Paid Account License	Fixed Monthly Fee Per Unit	None	Specific	3,972	$ 6.95	$ 27,605.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Video Streaming - COC Chambers	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 1,282.60	15391.20	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Video Streaming and Archiving Services	Schedule 4.3 - Section 5.10	Network Services	System	Fixed Monthly Fee Per Unit		Specific	12	$ 7,283.61	$ 87,403.32	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Engagement HQ	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 5,975.75	$ 71,709.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Legislative Management Suite	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 3,847.80	$ 46,173.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
VoteCast	Schedule 4.3 - Section 5.10	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 2,506.90	$ 30,082.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Mobile Devices Support Services - Intune	Schedule 4.3 - Section 4.8	End User Services	Device	Fixed Monthly Fee Per Unit		Specific	57,000	$7.89	$ 449,730.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Wireless Access Point	Schedule 4.3 - Section 5.12	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	8,808	$ 168.19	$ 1,481,417.52	$ 192.56	$ 179.96	$ 164.61	$ 161.04	$ 157.34	$ 153.88	3
Network Access - Wire/Wireless	Schedule 4.3 - Section 5.12	Network Services	Active Account	Fixed Monthly Fee Per Unit	B2	Specific	179,304	$ 68.86	$ 12,347,330.84	$ 78.84	$ 73.68	$ 67.49	$ 66.14	$ 64.81	$ 63.52	n/a
3rd-Party Network Access - Category 1	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	36	$ 548.07	$ 19,730.55	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd-Party Network Access - Category 2	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	24	$ 555.21	$ 13,324.93	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd-Party Network Access - Category 3	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	60	$ 568.32	$ 34,098.92	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - IP Sec - 5 Mbps	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	120	$ 255.85	$ 30,702.11	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - IP Sec - 10 Mbps	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 442.39	$ 5,308.67	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (1 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 153.51	$ 1,842.13	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (2 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 260.12	$ 3,121.38	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (3 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	24	$ 340.45	$ 8,170.79	n/a	n/a	n/a	n/a	n/a	n/a	5

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
3rd Party Network Access - Virtual Access (4 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 473.32	$ 5,679.89	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (5 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	36	$ 609.53	$ 21,943.16	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (6-10 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 1,166.54	$ 13,998.53	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (20 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 1,907.15	$ 1,907.15	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (30 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 2,504.79	$ 2,504.79	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (40 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 2,879.77	$ 2,879.77	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Virtual Access (50 Mbps)	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	1	$ 3,032.09	$ 3,032.09	n/a	n/a	n/a	n/a	n/a	n/a	5
3rd Party Network Access - Microsoft Teams Rooms	Schedule 4.3 - Section 5.13	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	168	$ 369.66	$ 62,102.88	n/a	n/a	n/a	n/a	n/a	n/a	n/a
External DNS Management	Schedule 4.3 - Section 5.14	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 15,275.83	$ 183,309.93	n/a	n/a	n/a	n/a	n/a	n/a	n/a
External DNS Management Enhancement	Schedule 4.3 - Section 5.14	Network Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 29,539.27	$ 354,471.24	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type I Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 244,519.76	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 12,846.12	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 8,460.96	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,207.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type I Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 49,159.13	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type II Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 122,259.84	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 11,118.13	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 8,460.96	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,207.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type II Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 24,579.56	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type III Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 84,706.98	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 11,118.13	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 8,460.96	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,207.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type III Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 12,289.78	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type IV Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 71,182.99	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
New Site Install - Type IV Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 9,390.14	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,434.81	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,207.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type IV Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 6,144.89	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type V Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 17,630.81	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 9,390.14	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,434.81	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,207.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type V Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 3,932.73	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install – Type VI Fixed Component	Schedule 4.3 - Section 5.16	Network Services	Install	Fixed Fee Per Unit		Cumulative	**	$ 3,356.91	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Main Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 6,364.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Intermediate Distribution Frame	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 5,434.81	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Backbone	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 23,207.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Type VI Variable Component - Project Manager	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 2,212.16	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
New Site Install - Cable Drops	Schedule 4.3 - Section 5.16	Network Services	Unit	Fixed Fee Per Unit		Cumulative	**	$ 526.31	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Large	Schedule 4.3 - Section 5.17	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	96	$ 8,646.33	$ 830,047.68	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Medium	Schedule 4.3 - Section 5.17	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	12	$ 2,858.63	$ 34,303.50	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Small	Schedule 4.3 - Section 5.17	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	348	$ 721.88	$ 251,212.50	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Interactive Voice Services - Support for County Retained	Schedule 4.3 - Section 5.17	Network Services	Network	Fixed Monthly Fee Per Unit		Specific	180	$ 638.68	$ 114,962.90	n/a	n/a	n/a	n/a	n/a	n/a	5
FirstNet Mobility Services	Schedule 4.3 - Section 5.18	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12,000	$33.06 ≥ 1000 per month	$ 396,720.00	$38.31 ≤ 999 per month	n/a	n/a	n/a	n/a	n/a	n/a
FirstNet Mobility Services - Tethered	Schedule 4.3 - Section 5.18	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12,000	$38.43 ≥ 1000 per month	$ 461,160.00	$43.68 ≤ 999 per month	n/a	n/a	n/a	n/a	n/a	n/a
Mobility Services Hot Spot	Schedule 4.3 - Section 5.18	Network Services	Device	Fixed Monthly Fee Per Unit		Specific	12	$ 26.85	$ 322.20	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Citrix Account	Schedule 4.3 - Section 6	Data Center Services	Account	Fixed Monthly Fee Per Unit		Specific	400	$ 20.68	$ 8,272.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Transaction	Schedule 4.3 - Section 6	Data Center Services	Third Party Transaction	Fixed Monthly Fee Per Unit		Cumulative	n/a	5% of invoice amount	**	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Wild Fire Scanning Service	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$6,658.80	$ 79,905.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Virtual Guest Server - Cloud IaaS	Schedule 4.3 - Section 6	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	48	53473%	$ 25,667.04	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Virtual Guest Server - Cloud PaaS	Schedule 4.3 - Section 6	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	48	$ 401.05	$ 19,250.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Clonetab Solution	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 6,211.24	$ 74,534.88	n/a	n/a	n/a	n/a	n/a	n/a	4
DIMSNET Solution	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 15,369.32	$ 184,431.84	n/a	n/a	n/a	n/a	n/a	n/a	$ 4.00
NetBackup Solution	Schedule 4.3 - Section 6	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 107,963.65	$ 1,295,563.80							
Mainframe	Schedule 4.3 - Section 6.6	Data Center Services	CPU Hour***	Fixed Monthly Fee Per Unit		Specific	15,305	$ 89.87	$ 1,375,397.56	n/a	n/a	n/a	n/a	n/a	n/a	7
AS/400	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	12	$ 2,962.73	$ 35,552.74	n/a	n/a	n/a	n/a	n/a	n/a	5
Copia Fax Line	Schedule 4.3 - Section 6.7	Data Center Services	Fax Line	Fixed Monthly Fee Per Unit		Specific	12	$ 125.00	$ 1,500.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Low Code Application Platform - OutSystems	Schedule 4.3 - Section 6.7	Data Center Services	User	Fixed Monthly Fee Per Unit		Specific	5,000	≤5000 $54.06	$ 270,300.00	n/a	n/a	>5000 $42.00	n/a	n/a	n/a	n/a
Oracle Exadata Services Backup and Recovery	Schedule 4.3 - Section 6.7	Data Center Services	Appliance	Fixed Monthly Fee Per Unit		Specific	0	$ 122.88	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata Services - Eighth Rack	Schedule 4.3 - Section 6.7	Data Center Services	Appliance	Fixed Monthly Fee Per Unit		Specific	12	$ 10,380.95	$ 124,571.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata X8M - Business Continuity	Schedule 4.3 - Section 6.7	Data Center Services	Appliance	Fixed Monthly Fee Per Unit		Specific	12	$ 41,268.64	$ 495,223.65	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata X8M - Development / Test	Schedule 4.3 - Section 6.7	Data Center Services	Appliance	Fixed Monthly Fee Per Unit		Specific	12	$ 33,503.21	$ 402,038.49	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Oracle Exadata X8M - Production	Schedule 4.3 - Section 6.7	Data Center Services	Appliance	Fixed Monthly Fee Per Unit		Specific	12	$ 40,951.09	$ 491,413.08	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Physical Server UNIX - Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	900	$ 4,537.06	$ 4,083,358.04	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server UNIX - Medium	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	720	$ 2,692.34	$ 1,938,483.61	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server UNIX - Small	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	330	$ 1,684.89	$ 556,014.02	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server UNIX - X-Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	72	$ 5,238.56	$ 377,176.32	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Unix - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	11	$ 4,628.27	$ 50,910.97	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Wintel - Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	160	$ 1,559.37	$ 249,499.95	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Wintel - Medium	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	300	$ 1,085.38	$ 325,614.33	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Wintel - Small	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	400	$874.58	$ 349,833.24	n/a	n/a	n/a	n/a	n/a	n/a	5
Physical Server Wintel - X-Large	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	24	$1,823.60	$ 43,766.40	n/a	n/a	n/a	n/a	n/a	n/a	4
Physical Server Wintel - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	2	$1,732.42	$ 3,464.84	n/a	n/a	n/a	n/a	n/a	n/a	4
Virtual Guest Server - Linux	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	300	$ 601.60	$ 180,480.64	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	63	$ 571.52	$ 36,005.76	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Unix	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	160	$ 1,203.20	$ 192,512.68	n/a	n/a	n/a	n/a	n/a	n/a	5
Virtual Guest Server - Unix - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	7	$ 1,143.04	$ 8,001.28	n/a	n/a	n/a	n/a	n/a	n/a	$ 5.00
Virtual Guest Server - Windows	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	4,550	$ 572.95	$ 2,606,942.52	n/a	n/a	n/a	n/a	n/a	n/a	$ 5.00
Virtual Guest Server - Windows - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	8	$ 544.31	$ 4,354.48	n/a	n/a	n/a	n/a	n/a	n/a	$ 5.00

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Virtual Host Server - Windows / Linux	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	160	$ 4,955.61	$ 792,897.17	n/a	n/a	n/a	n/a	n/a	n/a	$ 4.00
Virtual Host Server - Windows / Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Data Center Services	Server	Fixed Monthly Fee Per Unit		Specific	3	$ 4,707.83	$ 14,123.49	n/a	n/a	n/a	n/a	n/a	n/a	$ 4.00
Infrastructure Services	Schedule 4.3 - Section 6.8	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 335,063.58	$ 4,020,763.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Development & Test Services	Schedule 4.3 - Section 6.9	Data Center Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 235,207.11	$ 2,822,485.32	n/a	n/a	n/a	n/a	n/a	n/a	n/a
E-Mail Services	Schedule 4.3 - Section 6.10	Data Center Services	Active Account	Fixed Monthly Fee Per Unit		Specific	162,420	$ 5.23	$ 849,946.39	n/a	n/a	n/a	n/a	n/a	n/a	5
Attached Storage - AS/400	Schedule 4.3 - Section 6.7	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit		Specific	1,920	$ 0.695	$ 1,334.40	n/a	n/a	n/a	n/a	n/a	n/a	7
Attached Storage - Mainframe	Schedule 4.3 - Section 6.7	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit		Specific	13,286	$ 6.73	$ 89,414.78	n/a	n/a	n/a	n/a	n/a	n/a	7
Acclaim Riverbed	Schedule 4.3 - Section 6.8	Data Center Services	Riverbed	Fixed Monthly Fee Per Unit		Specific	72	$ 1,905.36	$ 137,185.92	n/a	n/a	n/a	n/a	n/a	n/a	4
Virtual Fax	Schedule 4.3 - Section 6.10	Data Center Services	Account	Fixed Monthly Fee Per Unit		Specific	500	$ 38.28	$ 19,140.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Attached Storage - WINTEL	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	38,826	$ 0.52	$ 20,189.52	$ 0.60	$ 0.55	$ 0.51	$ 0.50	$ 0.49	$ 0.48	n/a
Attached Storage - Unix	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	0	$ 0.73	$ -	$ 0.83	$ 0.77	$ 0.72	$ 0.70	$ 0.69	$ 0.68	n/a
Storage - Document Processing Center 1	Schedule 4.3 - Section 6.12	Data Center Services	Unit	Fixed Monthly Fee Per Unit		Specific	12	$ 17,408.16	$ 208,897.92	n/a	n/a	n/a	n/a	n/a	n/a	$ 5.00
Storage - Document Processing Center 2	Schedule 4.3 - Section 6.12	Data Center Services	Unit	Fixed Monthly Fee Per Unit		Specific	12	$ 10,319.400	$ 123,832.80	n/a	n/a	n/a	n/a	n/a	n/a	5
Storage - Archive Tier	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	0	$ 0.20	$ -	$ 0.22	$ 0.21	$ 0.19	$ 0.19	$ 0.19	$ 0.18	n/a
Storage - Primary Tier	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	1,638,468	$ 0.47	$ 770,079.96	$ 0.54	$ 0.50	$ 0.45	$ 0.44	$ 0.44	$ 0.43	n/a
Storage - Secondary Tier	Schedule 4.3 - Section 6.12	Data Center Services	Used Gigabyte	Fixed Monthly Fee Per Unit	B3	Specific	3,554,814	$ 0.32	$ 1,137,540.48	$ 0.37	$ 0.34	$ 0.30	$ 0.30	$ 0.29	$ 0.29	n/a
Storage - Immutable Tier (1TB)	Schedule 4.3 - Section 6.12	Data Center Services	1 Terabyte	Fixed Monthly Fee Per Unit		Specific	144	$ 355.57	$ 51,202.34	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Storage - Immutable Tier (500GB)	Schedule 4.3 - Section 6.12	Data Center Services	512 Gigabyte	Fixed Monthly Fee Per Unit		Specific	120	$ 177.79	$ 21,334.31	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBackup Solution Amazon Web Services	Schedule 4.3 - Section 6.13	Data Center Services	TB	Fixed Monthly Fee Per Unit		Specific	164	$ 86.31	$ 14,154.84	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Print per 1,000 images (Paper)	Schedule 4.3 - Section 6.14	Data Center Services	1000 Images	Fixed Fee Per Unit		Cumulative	4,318	$ 63.62	$ 274,719.02	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Microfiche Originals	Schedule 4.3 - Section 6.14	Data Center Services	Copy	Fixed Fee Per Unit		Cumulative	12,264	$ 1.20	$ 14,771.99	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Microfiche Duplicates	Schedule 4.3 - Section 6.14	Data Center Services	Copy	Fixed Fee Per Unit		Cumulative	41,964	$ 0.12	$ 4,846.84	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Fixed Price Applications Service Request	Exhibit 16.1	Applications Services	Service Request	Fixed Fee Per Unit		Cumulative	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Negotiation-Large	Exhibit 4.3 - Section 2.3.1.4, Exhibit 16.1	Cross Functional Services	Third Party Agreement	Fixed Fee Per Unit		Cumulative	**	$ 10,000.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Negotiation-Small	Exhibit 4.3 - Section 2.3.1.4, Exhibit 16.1	Cross Functional Services	Third Party Agreement	Fixed Fee Per Unit		Cumulative	**	$ 5,000.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Third Party Transaction	Exhibit 4.3 - Section 2.3.1.4, Exhibit 16.1	Cross Functional Services	Third Party Transaction	Fixed Fee Per Unit		Cumulative	**	3% - 5% (Depending on product or service)	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Optional Item Catalog (OIC) Software Addition	Exhibit 16.1 - Section 10.3	Catalog	Add	Fixed Fee Per Unit		Cumulative	12	$ 2,450.00	$ 29,400.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Optional Item Catalog (OIC) Hardware Addition	Exhibit 16.1 - Section 10.3	Catalog	Add	Fixed Fee Per Unit		Cumulative	12	$ 500.00	$ 6,000.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
Optional Item Catalog (OIC) - Update	Exhibit 16.1 - Section 10.2	Catalog	Update	Fixed Fee Per Unit		Cumulative	12	$ 1,470.00	$ 17,640.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Electronic Health Records Program Management Services	Schedule 4.3 - Section 7.4	Applications Services	Month	Fixed Monthly Fee Per Unit		Specific	12	$ 57,200.00	$ 686,400.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Acquisition Manager	Exhibit 4.3 - Section 2.3.1.5, Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	4,160	$ 132.50	$ 551,200.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Architect	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	9,685	$ 172.59	$ 1,671,536.22	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	11,497	$ 104.49	$ 1,201,302.87	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - Advanced Technology	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	88,864	$ 140.14	$ 12,453,165.71	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - Associate	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	283	$ 74.20	$ 20,998.60	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - ERP Principal	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	3,700	$ 195.00	$ 721,500.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Developer - Senior	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	42,938	$ 127.84	$ 5,489,391.54	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Test Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	3,783	$ 100.70	$ 380,948.10	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Test Lead	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,570	$ 133.98	$ 344,338.88	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Business Analyst	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,080	$ 120.59	$ 250,836.69	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Data Entry Clerk	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	400	$ 27.00	$ 10,800.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Desktop Engineer	Exhibit 16.1-4	End User Services	Hour	Fixed Fee Per Unit		Cumulative	400	$ 105.95	$ 42,380.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Database Administrator	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	20,545	$ 147.14	$ 3,023,078.01	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Gate Review Coordinator	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	160	$ 95.40	$ 15,264.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Information Security Engineer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	4,800	$ 175.00	$ 840,000.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Innovation Core Team Member (Effective CY2)	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	**	$ 178.95	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Intern	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	800	$ 34.00	$ 27,200.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Junior Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	400	$ 34.00	$ 13,600.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Network Architect	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	120	$ 179.54	$ 21,544.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Network Engineer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	120	$ 115.95	$ 13,914.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Network Engineer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	120	$ 160.67	$ 19,280.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Curam Application Developer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	4,160	$ 206.70	$ 859,872.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Curam Business Analyst	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,080	$ 196.10	$ 407,888.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Senior Curam Interface Architect	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,080	$ 275.60	$ 573,248.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Technology Transition and Adoption Coordinator	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,040	168	$ 342,720.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Program Manager	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	897	206	$ 184,364.70	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Project Manager	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	19,785	165	$ 3,257,825.59	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Project Scheduler	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	1,494	$ 100.70	$ 150,445.80	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Systems Analyst	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	29,295	$ 121.70	$ 3,565,149.57	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Web Designer	Exhibit 16.1-4	Applications Services	Hour	Fixed Fee Per Unit		Cumulative	2,449	$ 112.85	$ 276,363.40	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Applications Maintenance & Operations FFP (County)	Exhibit 16.1-5b	Applications Services	Year	Fixed Fee Per Unit		Specific	**		$ 9,703,687.27	n/a	n/a	n/a	n/a	n/a	n/a	n/a
ARCC Special Service Level Support Services - Event Coverage	Schedule 4.8-1	Special Service Level Requirements	Event	Fixed Fee Per Unit		Specific	22	$ 2,877.33	$ 63,301.16	n/a	n/a	n/a	n/a	n/a	n/a	n/a
ARCC Special Service Level Support Services - Daily Support	Schedule 4.8-1	Special Service Level Requirements	Day	Fixed Fee Per Unit		Cumulative	5	$ 1,438.66	$ 7,193.31	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Registrar of Voters	Schedule 4.8-1	Special Service Level Requirements	Day	Fixed Fee Per Unit		Cumulative	99	$ 455.07	$ 45,051.93	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Tax Sale Event	Schedule 4.8-1	Special Service Level Requirements	Event	Fixed Fee Per Unit		Specific	1	$ 5,921.21	$ 5,921.21	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Tax Collection Event	Schedule 4.8-1	Special Service Level Requirements	Event	Fixed Fee Per Unit		Specific	2	$ 11,866.99	$ 23,733.98	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Service Level Special Requirements - Special Support Daily Coverage	Schedule 4.8-1	Special Service Level Requirements	Day	Fixed Fee Per Unit		Cumulative	50	$ 185.40	$ 9,270.00	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Labor	Schedule 4.3 - Section 2.17	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	0	$ 22,621.27	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Infrastructure	Schedule 4.3 - Section 2.17	Cross Functional Services	Month	Fixed Monthly Fee Per Unit		Specific	0	$ 56,744.73	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Small Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 55.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-6 Resource Unit Price Summary Option Term

Resource Unit (RU)	*Reference	Framework	Unit of Measure	Pricing Method	Bundle	Measurement Method	Baseline Volumes (per Contract Year)	RU Fee (90-110% band)	Baseline Annual Fee	RU Fee (70% to 80% band)	RU Fee (80% to 90% band)	RU Fee (110% to 120% band)	RU Fee (120% to 130% band)	RU Fee (130% to 150% band)	RU Fee (150% to 200% band)	Depreciation Period (in Years)
DR Medium Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 100.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Large Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 387.48	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR X-Large Windows/Linux - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 483.31	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Medium Solaris - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 193.14	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Large Solaris - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 556.21	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR X-Large Solaris - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	1 Terabyte	Fixed Monthly Fee Per Unit		Specific	0	$ 669.29	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR VTL Based Storage - 72 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 139.39	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Small Virtual - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 128.22	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Medium Virtual - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 144.19	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR Large Virtual - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 171.78	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DR 3PAR Based Storage - 48 Hour RTO	Schedule 4.3 - Section 2.17	Cross Functional Services	1 Terabyte	Fixed Monthly Fee Per Unit		Specific	0	$ 264.02	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 1 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 706.75	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 3 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 1,078.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 10 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 1,562.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond25 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 2,051.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 40 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 2,541.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 100 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 3,605.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 155 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 4,006.75	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 300 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 4,664.00	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 600 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 5,274.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 800 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 6,913.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 1000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 7,818.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 2000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 11,786.50	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 3000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 17,679.75	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 4000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 19,027.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
NetBond 5000 Mbps	n/a	n/a	Circuit	Fixed Monthly Fee Per Unit		Specific	0	$ 20,974.25	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Enterprise Information Management	n/a	n/a	Quantity	Fixed Fee Per Unit		Specific	0	$ 875,565.65	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Office 365 Network Enabler	n/a	n/a	Quantity	Fixed Monthly Fee Per Unit		Specific	0	$ 184,016.01	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Standard CATA Review	n/a	n/a	Quantity	Fixed Fee Per Unit		Specific	0	$ 56,716.23	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Delta CATA Review	n/a	n/a	Quantity	Fixed Fee Per Unit		Specific	0	$ 28,358.11	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
CATA Strategist	n/a	n/a	Hour	Fixed Fee Per Unit		Cumulative	0	$ 247.84	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Exhibit 16.1-6 Resource Unit Price Summary Option Term																
Resource Unit (RU)	***Reference**	**Framework**	**Unit of Measure**	**Pricing Method**	**Bundle**	**Measurement Method**	**Baseline Volumes (per Contract Year)**	**RU Fee (90-110% band)**	**Baseline Annual Fee**	**RU Fee (70% to 80% band)**	**RU Fee (80% to 90% band)**	**RU Fee (110% to 120% band)**	**RU Fee (120% to 130% band)**	**RU Fee (130% to 150% band)**	**RU Fee (150% to 200% band)**	**Depreciation Period (in Years)**
CATA Master	n/a	n/a	Hour	Fixed Fee Per Unit		Cumulative	0	$ 194.90	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
CATA Expert	n/a	n/a	Hour	Fixed Fee Per Unit		Cumulative	0	$ 159.67	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Oracle on Solaris - Onboarding	n/a	n/a	Server	Fixed Fee Per Unit		Specific	0	$ 120,017.07	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Oracle on Solaris - MRC for Service	n/a	n/a	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 34,323.54	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Oracle on Solaris - MRC per Instance Provisioned	n/a	n/a	Instance	Fixed Monthly Fee Per Unit		Specific	0	$ 35.72	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Public Cloud Provisioning - Onboarding	n/a	n/a	Instance	Fixed Fee Per Unit		Specific	0	$ 5,435.82	$ -		n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Public Cloud Provisioning - MRC for service	n/a	n/a	Server	Fixed Monthly Fee Per Unit		Specific	0	$ 51,913.91	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a
HMCB for Public Cloud Provisioning - MRC per instance provisioned	n/a	n/a	Instance	Fixed Monthly Fee Per Unit		Specific	0	$ 35.72	$ -	n/a	n/a	n/a	n/a	n/a	n/a	n/a

*Schedule 4.3 Reference includes the Section reference for the specific requirements for this particular Resource Unit but it still includes all general requirements applicable to such Resource Unit in the higher levels of the obligations hierarchy as described in Schedule 4.3. For example, the Resource Unit for Desktop - Standard Workstation includes not only the responsibilities as stated in Section 4.5 of the End-User Services Section of Schedule 4.3, but also the responsibilities in Sections 4.1 through 4.3 of the End-User Services Section, as well as the responsibilities and requirements in Section 1 of Schedule 4.3.
**Baseline volume is undetermined at this time
*** The mainframe RU unit volumes are based on the R24 CPUs
****With the exception of 2.3.1.4 and 2.3.1.5, and their respective requirements

Exhibit 16.1-6a – Resource Unit Price Decomposition Option Term

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Resource Unit (RU)	*Reference	Unit of Measure	Pricing Method	*Decomposition*	Resource Unit Fee Option Term	Component Fee Option Term	Component Description
Contract and Acquisition Management Services	***Schedule 4.3 - Section 2.3	Month	Fixed Monthly Fee Per Unit		$ 222,400.64		
				Service Desk Services		$ 5,972.82	Represents the portion of Contract Management labor attributable to providing Service Desk Services.
				End User Services		$ 36,675.33	Represents the portion of Contract Management labor attributable to providing End User Services.
				Network Services		$ 71,688.93	Represents the portion of Contract Management labor attributable to providing Network Services.
				Data Center Services		$ 32,266.69	Represents the portion of Contract Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 26,049.27	Represents the portion of Contract Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 49,747.61	Represents the portion of Contract Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 222,400.64	Represents the labor to support Contract and Acquisition Management Services as defined in Schedule 4.3, Section 2.3.
Integrated Asset Management Services	Schedule 4.3 - Section 2.4	Month	Fixed Monthly Fee Per Unit		$ 118,445.02		
				Service Desk Services		$ 3,180.97	Represents the portion of Asset Management labor attributable to providing Service Desk Services.
				End User Services		$ 19,532.36	Represents the portion of Asset Management labor attributable to providing End User Services.
				Network Services		$ 38,179.73	Represents the portion of Asset Management labor attributable to providing Network Services.
				Data Center Services		$ 17,184.43	Represents the portion of Asset Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 13,873.19	Represents the portion of Asset Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 26,494.33	Represents the portion of Asset Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 118,445.02	Represents the labor to support Integrated Asset Management Services as defined in Schedule 4.3, Section 2.4.
Billing Management Services	Schedule 4.3 - Section 2.5	Month	Fixed Monthly Fee Per Unit		$ 43,985.05		
				Service Desk Services		$ 1,181.27	Represents the portion of Billing Management labor attributable to providing Service Desk Services.
				End User Services		$ 7,253.42	Represents the portion of Billing Management labor attributable to providing End User Services.
				Network Services		$ 14,178.20	Represents the portion of Billing Management labor attributable to providing Network Services.
				Data Center Services		$ 6,381.51	Represents the portion of Billing Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 5,151.87	Represents the portion of Billing Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 9,838.78	Represents the portion of Billing Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 43,985.05	Represents the labor to support Billing Management Services as defined in Schedule 4.3, Section 2.5.
Security Management Services	Schedule 4.3 - Section 2.6	Month	Fixed Monthly Fee Per Unit		$ 252,784.50		
				Service Desk Services		$ 7,608.62	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Service Desk Services.
				End User Services		$ 46,719.78	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of End User Services.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Network Services		$ 60,796.65	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Network Services.
				Data Center Services		$ 41,103.72	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Data Center Services.
				Application Maintenance & Operations Services		$ 33,183.50	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Applications Maintenance & Operations Services.
				Application Development Services		$ 63,372.23	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Security Management services in support of Application Development Services.
				Hardware		$ -	N/A
				Software		$ 2,790.78	Represents Software tools to support the County Environment.
				Labor		$ 249,993.72	Represents the labor to support Security Management Services as defined in Schedule 4.3, Section 2.6.
Malware Protection	Schedule 4.3 - Section 6.26	Month	Fixed Monthly Per Unit		$ 5,270.06		
				Hardware		$ -	
				Software		$ 2,927.81	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	N/A
				Software Support		$ 2,342.25	Vendor and ITO on-going support of County requirement changes; modifications after the initial integration and Production Support
Secure Internet Access	Schedule 4.3 - Section 6.26	Month	Fixed Monthly Per Unit		$ 28,211.10		
				Hardware		$ -	N/A
				Software		$ 18,218.72	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	N/A
				Software Support		$ 9,992.38	Vendor and ITO on-going support of County requirement changes; modifications after the initial integration and Production Support
Multi-Factor Authentication Service	Schedule 4.3 Section 2.6	Month	Fixed Monthly Per Unit		$ 43,883.82		
				Hardware		$ -	
				Operating System License		$ -	
				Other Software License		$ 23,424.42	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	
				Software Maintenance		$ 20,459.40	Represents costs associated with software maintenance along with the labor and resources for support by vendor and Contractor.
Service Delivery Management Services	Schedule 4.3 - Section 2.7	Month	Fixed Monthly Fee Per Unit		$ 207,383.46		
				Service Desk Services		$ 6,687.29	Represents the portion of Service Delivery Management labor attributable to providing Service Desk Services.
				End User Services		$ 41,062.48	Represents the portion of Service Delivery Management labor attributable to providing End User Services.
				Network Services		$ 38,643.40	Represents the portion of Service Delivery Management labor attributable to providing Network Services.
				Data Center Services		$ 36,126.47	Represents the portion of Service Delivery Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 29,165.32	Represents the portion of Service Delivery Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 55,698.49	Represents the portion of Service Delivery Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 207,383.46	Represents the labor to support SDM Services as defined in Schedule 4.3, Section 2.7.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Project Management Services	Schedule 4.3 - Section 2.9	Month	Fixed Monthly Fee Per Unit		$ 140,665.48		
				Service Desk Services		$ 3,777.73	Represents the portion of Project Management labor attributable to providing Service Desk Services.
				End User Services		$ 23,196.66	Represents the portion of Project Management labor attributable to providing End User Services.
				Network Services		$ 45,342.31	Represents the portion of Project Management labor attributable to providing Network Services.
				Data Center Services		$ 20,408.25	Represents the portion of Project Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 16,475.82	Represents the portion of Project Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 31,464.71	Represents the portion of Project Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 140,665.48	Represents the labor to support Project Management Services as defined in Schedule 4.3, Section 2.9.
Integration and Testing Services	Schedule 4.3 - Section 2.10	Month	Fixed Monthly Fee Per Unit		$ 38,164.21		
				Service Desk Services		$ 1,024.94	Represents the portion of Integration and Testing labor attributable to providing Service Desk Services.
				End User Services		$ 6,293.53	Represents the portion of Integration and Testing labor attributable to providing End User Services.
				Network Services		$ 12,301.90	Represents the portion of Integration and Testing labor attributable to providing Network Services.
				Data Center Services		$ 5,537.00	Represents the portion of Integration and Testing labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 4,470.08	Represents the portion of Integration and Testing labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 8,536.75	Represents the portion of Integration and Testing labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 38,164.21	Represents the labor to support Integrated and Testing Services as defined in Schedule 4.3, Section 2.10.
Incident Management Services	Schedule 4.3 - Section 2.11	Month	Fixed Monthly Fee Per Unit		$ 3,482.29		
				Service Desk Services		$ 93.52	Represents the portion of Incident Management labor attributable to providing Service Desk Services.
				End User Services		$ 574.25	Represents the portion of Incident Management labor attributable to providing End User Services.
				Network Services		$ 1,122.49	Represents the portion of Incident Management labor attributable to providing Network Services.
				Data Center Services		$ 505.22	Represents the portion of Incident Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 407.87	Represents the portion of Incident Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 778.93	Represents the portion of Incident Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 3,482.29	Represents the labor to support Incident Management Services as defined in Schedule 4.3, Section 2.11.
Problem Management Services	Schedule 4.3 - Section 2.12	Month	Fixed Monthly Fee Per Unit		$ 3,482.29		
				Service Desk Services		$ 93.52	Represents the portion of Problem Management labor attributable to providing Service Desk Services.
				End User Services		$ 574.25	Represents the portion of Problem Management labor attributable to providing End User Services.
				Network Services		$ 1,122.49	Represents the portion of Problem Management labor attributable to providing Network Services.
				Data Center Services		$ 505.22	Represents the portion of Problem Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 407.87	Represents the portion of Problem Management labor attributable to providing Application Maintenance & Operations Services.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Application Development Services		$ 778.93	Represents the portion of Problem Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 3,482.29	Represents the labor to support Problem Management Services as defined in Schedule 4.3, Section 2.12.
Change Management Services	Schedule 4.3 - Section 2.13	Month	Fixed Monthly Fee Per Unit		$ 9,776.47		
				Service Desk Services		$ 262.56	Represents the portion of Change Management labor attributable to providing Service Desk Services.
				End User Services		$ 1,612.20	Represents the portion of Change Management labor attributable to providing End User Services.
				Network Services		$ 3,151.36	Represents the portion of Change Management labor attributable to providing Network Services.
				Data Center Services		$ 1,418.41	Represents the portion of Change Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 1,145.10	Represents the portion of Change Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 2,186.85	Represents the portion of Change Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 9,776.47	Represents the labor to support Change Management Services as defined in Schedule 4.3, Section 2.13.
Release Management Services	Schedule 4.3 - Section 2.14	Month	Fixed Monthly Fee Per Unit		$ 11,001.46		
				Service Desk Services		$ 295.46	Represents the portion of Release Management labor attributable to providing Service Desk Services.
				End User Services		$ 1,814.21	Represents the portion of Release Management labor attributable to providing End User Services.
				Network Services		$ 3,546.23	Represents the portion of Release Management labor attributable to providing Network Services.
				Data Center Services		$ 1,596.13	Represents the portion of Release Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 1,288.58	Represents the portion of Release Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 2,460.86	Represents the portion of Release Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 11,001.46	Represents the labor to support Release Management Services as defined in Schedule 4.3, Section 2.14.
Configuration Management	Schedule 4.3 - Section 2.15	Month	Fixed Monthly Fee Per Unit		$ 18,978.04		
				Service Desk Services		$ 509.68	Represents the portion of Configuration Management labor attributable to providing Service Desk Services.
				End User Services		$ 3,129.60	Represents the portion of Configuration Management labor attributable to providing End User Services.
				Network Services		$ 6,117.41	Represents the portion of Configuration Management labor attributable to providing Network Services.
				Data Center Services		$ 2,753.40	Represents the portion of Configuration Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 2,222.85	Represents the portion of Configuration Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 4,245.10	Represents the portion of Configuration Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 18,978.04	Represents the labor to support Configuration Management Services as defined in Schedule 4.3, Section 2.15.
Capacity Planning and Performance Management Services	Schedule 4.3 - Section 2.16	Month	Fixed Monthly Fee Per Unit		$ 18,372.67		
				Service Desk Services		$ -	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Service Desk Services.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				End User Services		$ 3,029.77	Represents the portion of Capacity Planning and Performance Management labor attributable to providing End User Services.
				Network Services		$ 5,922.27	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Network Services.
				Data Center Services		$ 2,665.57	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 2,151.95	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 4,109.68	Represents the portion of Capacity Planning and Performance Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 18,372.67	Represents the labor to support Capacity Planning and Performance Management Services as defined in Schedule 4.3, Section 2.16.
Disaster Recovery Management Services	Schedule 4.3 - Section 2.17	Month	Fixed Monthly Fee Per Unit		$ 194,230.46		
				Service Desk Services		$ 97.12	Represents the labor required to manage, update and test the Disaster Recovery Plan for Service Desk Services.
				End User Services		$ 194.23	Represents the labor required to manage and update Disaster Recovery Plan documents for End User Services. This includes providing input to County Business Continuity Plans and supporting testing as needed.
				Network Services		$ 38,846.09	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Network Disaster Recovery Services.
				Data Center Services		$ 145,381.50	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Data Center Disaster Recovery Services.
				Application Maintenance & Operations Services		$ 9,711.52	Represents the labor required to manage, update and test the Technical Recovery Plans for individual Applications, within the scope of the Data Center Disaster Recovery Plan.
				Application Development Services		$ -	N/A
				Hardware		$ 115,817.70	Represents the servers routers, switches, and storage equipment required to support DR environment.
				Software		$ 31,898.01	Represents the software costs associated with DR hardware used to support the DR environment.
				Labor		$ 46,514.75	Represents the labor to support Disaster Recovery Management Services as defined in Schedule 4.3, Section 2.17.
Identity Access Management Services	Schedule 4.3 - Section 2.18	Month	Fixed Monthly Fee Per Unit		$ 137,432.70		
				Service Desk Services		$ 3,690.91	Represents the portion of Identity Access Management labor attributable to providing Service Desk Services.
				End User Services		$ 22,663.56	Represents the portion of Identity Access Management labor attributable to providing End User Services.
				Network Services		$ 44,300.25	Represents the portion of Identity Access Management labor attributable to providing Network Services.
				Data Center Services		$ 19,939.23	Represents the portion of Identity Access Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 16,097.17	Represents the portion of Identity Access Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 30,741.59	Represents the portion of Identity Access Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ 22,070.21	Includes Symantec PKI Maintenance and Tools for IDAM resources to support the County environment.
				Labor		$ 115,362.49	Represents the labor to support Identity Access Management Services as defined in Schedule 4.3, Section 2.18.
Reporting Management Services	Schedule 4.3 - Section 2.19	Month	Fixed Monthly Fee Per Unit		$ 77,693.51		
				Service Desk Services		$ 2,086.55	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Service Desk Services.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				End User Services		$ 12,812.17	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of End User Services.
				Network Services		$ 25,043.83	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Network Services.
				Data Center Services		$ 11,272.05	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Data Center Services.
				Application Maintenance & Operations Services		$ 9,100.06	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Applications Maintenance & Operations Services.
				Application Development Services		$ 17,378.85	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Reporting Management services in support of Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 77,693.51	Represents the labor to support Reporting Management Services as defined in Schedule 4.3, Section 2.19.
Domain Name Management Services	Schedule 4.3 - Section 2.20	Month	Fixed Monthly Fee Per Unit		$ 1,599.85		
				Service Desk Services			N/A
				End User Services			N/A
				Network Services		$ 1,599.85	Represents the portion of Domain Name Management labor attributable to providing Network Services.
				Data Center Services			N/A
				Application Maintenance & Operations Services			N/A
				Application Development Services			N/A
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 1,599.85	Represents the labor to support Domain Name Management Services as defined in Schedule 4.3, Section 2.20.
Business Analyst Services	Schedule 4.3 - Section 2.21	Month	Fixed Monthly Fee Per Unit		$ 83,261.44		
				Service Desk Services		$ 3,134.73	Represents the portion of Business Analyst Services labor attributable to providing Service Desk Services.
				End User Services		$ 19,248.40	Represents the portion of Business Analyst Services labor attributable to providing End User Services.
				Network Services		$ 4,163.07	Represents the portion of Business Analyst Services labor attributable to providing Network Services.
				Data Center Services		$ 16,934.60	Represents the portion of Business Analyst Services labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 13,671.50	Represents the portion of Business Analyst Services labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 26,109.15	Represents the portion of Business Analyst Services labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 83,261.44	Represents the labor to support Business Analyst Services as defined in Schedule 4.3, Section 2.21.
Chief Technical Architect Services	Schedule 4.3 - Section 2.22	Month	Fixed Monthly Fee Per Unit		$ 19,097.64		
				Service Desk Services		$ 3,182.94	Represents the portion of CTA labor attributable to providing Service Desk Services.
				End User Services		$ 3,182.94	Represents the portion of CTA labor attributable to providing End User Services.
				Network Services		$ 3,182.94	Represents the portion of CTA labor attributable to providing Network Services.
				Data Center Services		$ 3,182.94	Represents the portion of CTA labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 3,182.94	Represents the portion of CTA labor attributable to providing Application Maintenance & Operations Services.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Application Development Services		$ 3,182.94	Represents the portion of CTA labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 19,097.64	Represents the labor to support CTA Services as defined in Schedule 4.3, Section 2.22.
Enterprise Applications Architect Services	Schedule 4.3 - Section 2.23	Month	Fixed Monthly Fee Per Unit		$ 19,097.64		
				Service Desk Services		$ 3,182.94	Represents the portion of EAA labor attributable to providing Service Desk Services.
				End User Services		$ 3,182.94	Represents the portion of EAA labor attributable to providing End User Services.
				Network Services		$ 3,182.94	Represents the portion of EAA labor attributable to providing Network Services.
				Data Center Services		$ 3,182.94	Represents the portion of EAA labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 3,182.94	Represents the portion of EAA labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 3,182.94	Represents the portion of EAA labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 19,097.64	Represents the labor to support EAA Services as defined in Schedule 4.3, Section 2.23.
Innovation Management Services	Schedule 4.3 - Section 2.24	Month	Fixed Monthly Fee Per Unit		$ 21,073.13		
				Service Desk Services		$ 3,512.19	Represents the portion of Innovation Management labor attributable to providing Service Desk Services.
				End User Services		$ 3,512.19	Represents the portion of Innovation Management labor attributable to providing End User Services.
				Network Services		$ 3,512.19	Represents the portion of Innovation Management labor attributable to providing Network Services.
				Data Center Services		$ 3,512.19	Represents the portion of Innovation Management labor attributable to providing Data Center Services.
				Application Maintenance & Operations Services		$ 3,512.19	Represents the portion of Innovation Management labor attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 3,512.19	Represents the portion of Innovation Management labor attributable to providing Application Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 21,073.13	Represents the labor to support Innovation Management Services as defined in Schedule 4.3, Section 2.24.
Service Desk Services	Section 3.0	Month	Fixed Monthly Fee Per Unit		$ 184,350.93		
				Service Desk Services		$ 4,950.95	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Service Desk Services.
				End User Services		$ 30,400.68	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support End User Services.
				Network Services		$ 59,423.94	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Network Services.
				Data Center Services		$ 26,746.30	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support Data Center Services.
				Application Maintenance & Operations Services		$ 21,592.59	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support App Maintenance Services.
				Application Development Services		$ 41,236.47	Represents the portion of Labor, Hardware, Software and Other Direct Costs to support App Development Services.
				Hardware		$ -	N/A
				Software		$ -	N/A
				Labor		$ 184,350.93	Represents the labor to support Service Desk Services as defined in Schedule 4.3, Section 2.3.
Duo Hardware Token MFA	Schedule 4.3 - Section 4.5.2	Account	Fixed Monthly Fee Per Unit		$ 5.28		
				Hardware		$ -	N/A
				Software License		$ 2.76	Represents the cost of software license subscription.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				IMARS		$ 2.15	Represents labor costs for IMAR activities, Tier 1 Helpdesk.
Electronic Signature	Schedule 4.3 - Section 4.5.2	Transaction	Fixed Fee Per Unit		$ 1.01		
				Hardware		$ -	N/A
				Hardware (Refresh Labor)		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ -	N/A
				Software Maintenance		$ 0.81	Represents the cost associated to the software maintenance and labor costs.
				IMAR's		$ 0.01	Represents the cost associated to the IMAR labor.
				Service Desk		$ 0.19	Represents costs associated with Service Desk labor.
Desktop - 3D Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 254.53		
				Hardware		$ 134.91	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 25.02	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 26.70	Represents break-fix services, primarily labor and parts.
				Software License		$ 20.00	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 36.71	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 10.03	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 1.17	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Advanced Engineering Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 195.52		
				Hardware		$ 111.60	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 17.60	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 18.82	Represents break-fix services, primarily labor and parts.
				Software License		$ 14.07	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 25.80	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 7.11	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.53	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Advanced Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 87.52		
				Hardware		$ 46.39	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 8.60	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 9.18	Represents break-fix services, primarily labor and parts.
				Software License		$ 6.88	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 12.62	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.45	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.40	Represents the labor associated with maintaining the Desktop Application Directory.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Desktop - Engineering Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 103.35		
				Hardware		$ 60.09	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 9.97	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 7.33	Represents break-fix services, primarily labor and parts.
				Software License		$ 6.95	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 15.17	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.32	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.52	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Gold Engineering Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 295.72		
				Hardware		$ 205.48	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 18.92	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 20.24	Represents break-fix services, primarily labor and parts.
				Software License		$ 15.13	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 27.74	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 7.64	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.57	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Mini Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 60.41		
				Hardware		$ 28.42	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 5.58	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 4.94	Represents break-fix services, primarily labor and parts.
				Software License		$ 5.63	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 13.52	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 1.86	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.46	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Scanner	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 139.09		
				Hardware		$ 107.38	Represents the costs of acquiring the asset, including feeder consumable kit. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 3.19	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 24.63	Represents break-fix services, primarily labor and parts, including annual preventive maintenance.
				Software License		$ -	N/A
				Software Maintenance		$ -	N/A
				IMAR's		$ 3.89	Represents labor costs for IMAR activities.
Desktop - Small Form Factor with Optical Drive	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 60.41		

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware		$ 28.42	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 5.58	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 4.94	Represents break-fix services, primarily labor and parts.
				Software License		$ 5.63	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 13.52	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 1.86	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.46	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - Standard Workstation	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Fee Per Unit		$ 60.41		
				Hardware		$ 28.42	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 5.58	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 4.94	Represents break-fix services, primarily labor and parts.
				Software License		$ 5.63	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 13.52	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 1.86	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.46	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Engineering	Schedule 4.3 - Section 4.5.3	Device	Fixed monthly fee per unit		$ 156.01		
				Hardware		$ 82.84	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 15.35	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 16.42	Represents break-fix services, primarily labor and parts.
				Software License		$ 12.23	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 22.59	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 6.17	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.41	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Ruggedized	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 175.15		
				Hardware		$ 112.28	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 10.48	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 9.86	Represents break-fix services, primarily labor and parts.
				Software License		$ 16.09	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 22.43	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.49	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.53	Represents the labor associated with maintaining the Desktop Application Directory.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Laptop - Standard	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 80.49		
				Hardware	[redacted]	$ 37.58	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)	[redacted]	$ 7.36	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance	[redacted]	$ 4.96	Represents break-fix services, primarily labor and parts.
				Software License	[redacted]	$ 11.52	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance	[redacted]	$ 16.14	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's	[redacted]	$ 2.45	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance	[redacted]	$ 0.48	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Standard LTE	Schedule 4.3 - Section 4.5.3	Device	Fixed monthly fee per unit		$ 100.90		
				Hardware	[redacted]	$ 53.58	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)	[redacted]	$ 9.93	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance	[redacted]	$ 10.61	Represents break-fix services, primarily labor and parts.
				Software License	[redacted]	$ 7.92	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance	[redacted]	$ 14.61	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's	[redacted]	$ 4.00	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance	[redacted]	$ 0.26	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Ultra Portable	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 87.29		
				Hardware	[redacted]	$ 42.03	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)	[redacted]	$ 7.51	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance	[redacted]	$ 7.10	Represents break-fix services, primarily labor and parts.
				Software License	[redacted]	$ 11.58	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance	[redacted]	$ 16.05	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's	[redacted]	$ 2.50	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance	[redacted]	$ 0.52	Represents the labor associated with maintaining the Desktop Application Directory.
Laptop - Ultra Portable 2in1	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 99.03		
				Hardware	[redacted]	$ 47.69	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)	[redacted]	$ 8.57	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance	[redacted]	$ 8.05	Represents break-fix services, primarily labor and parts.
				Software License	[redacted]	$ 13.14	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance	[redacted]	$ 18.20	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's	[redacted]	$ 2.86	Represents labor costs for IMAR activities.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Desktop Application Directory Maintenance		$ 0.52	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Convertible	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 88.61		
				Hardware		$ 47.15	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 6.79	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 6.50	Represents break-fix services, primarily labor and parts.
				Software License		$ 10.61	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 14.82	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.26	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.47	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Ruggedized	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 195.14		
				Hardware		$ 129.90	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 10.64	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 10.23	Represents break-fix services, primarily labor and parts.
				Software License		$ 16.69	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 23.60	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 3.55	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.53	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Surface Pro	Schedule 4.3 - Section 4.5.3	Device	Fixed Monthly Per Unit		$ 99.43		
				Hardware		$ 52.91	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 7.47	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 7.30	Represents break-fix services, primarily labor and parts.
				Software License		$ 11.90	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 16.83	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 2.49	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.53	Represents the labor associated with maintaining the Desktop Application Directory.
Tablet - Surface Pro LTE	Schedule 4.3 - Section 4.5.3	Device	Fixed monthly fee per unit		$ 127.64		
				Hardware		$ 67.77	Represents the costs of acquiring the asset. The component fee is the monthly lease payments for a leasing term of 3 years.
				Hardware (Refresh Labor)		$ 12.56	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 13.43	Represents break-fix services, primarily labor and parts.
				Software License		$ 10.01	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 18.48	Represents costs associated with the labor and resources for Software Maintenance support.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				IMAR's		$ 5.06	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.34	Represents the labor associated with maintaining the Desktop Application Directory.
County Retained Device	Schedule 4.3 - Section 4.7.3	Device	Fixed Monthly Per Unit		$ 95.87		
				Software License		$ 11.48	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 16.23	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 67.65	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.51	Represents the labor associated with maintaining the Desktop Application Directory.
Desktop - DCSS	Schedule 4.3 - Section 4.7.3	Device	Fixed Monthly Per Unit		$ 33.69		
				Hardware (Refresh Labor)		$ 3.13	Represents the labor for providing support for refresh tasks, on a 4-year cycle.
				Hardware Maintenance		$ 5.40	Represents break-fix services, primarily labor and parts.
				Software License		$ 5.05	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 9.71	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 8.13	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.50	Represents the labor associated with maintaining the Desktop Application Directory.
				Printer Maintenance		$ 1.78	Represents Level 2 printer support.
Laptop - DCSS	Schedule 4.3 - Section 4.7.3	Device	Fixed Monthly Per Unit		$ 41.21		
				Hardware (Refresh Labor)		$ 3.13	Represents the labor for providing support for refresh tasks, on a 3-year cycle.
				Hardware Maintenance		$ 6.73	Represents break-fix services, primarily labor and parts.
				Software License		$ 6.18	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 3 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Software Maintenance		$ 12.21	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR's		$ 10.13	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ 0.63	Represents the labor associated with maintaining the Desktop Application Directory.
				Printer Maintenance		$ 2.21	Represents Level 2 printer support.
Mobile Devices Support Services - Intune	Section 4.8	Device	Fixed Monthly Fee Per Unit		$ 7.89		
				Software License		$ -	Represents the costs of AirWatch software licenses upgrades/refresh. The aggregated cost is apportioned over the volume of Mobile Devices.
				Software Maintenance		$ 2.04	Represents costs associated with the labor and resources for Level 2 support and centralized hosting costs for Mobile Services applications.
				IMAR's		$ 5.85	Represents labor costs for IMAR activities.
				Desktop Application Directory Maintenance		$ -	N/A
Printer - Color Network Workgroup - Large Format (CNWP-LF)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 154.16		
				Hardware		$ 80.90	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 3.08	Represents the labor to install and refresh hardware amortized over the estimated asset life.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware Maintenance		$ 67.32	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 2.86	Represents labor costs for IMAR activities.
Printer - Color Network Workgroup - Standard Format (CNWP)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 62.84		
				Hardware		$ 38.01	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 0.94	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 21.70	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 2.19	Represents labor costs for IMAR activities.
Printer - Monochrome Network Workgroup - Standard Format (MNWP)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 56.25		
				Hardware		$ 33.82	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 1.13	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 20.29	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 1.02	Represents labor costs for IMAR activities.
Printer - Monochrome Network Workgroup - Large Format (MNWP-LF)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 90.61		
				Hardware		$ 62.58	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 1.81	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 24.77	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 1.45	Represents labor costs for IMAR activities.
Printer - Monochrome Network High Volume - Large Format (MNWP-LF-H)	Schedule 4.3 - Section 4.11.3	Device	Fixed Monthly Fee Per Unit		$ 147.76		
				Hardware		$ 94.09	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 2.19	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Hardware Maintenance		$ 45.36	Represents break-fix services, primarily labor and parts.
				IMAR's		$ 6.13	Represents labor costs for IMAR activities.
Electronic File Sharing Services	Schedule 4.3 -- Section 4.12	User	Fixed Monthly Fee Per Unit		$ 81.25		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 37.26	Represents the license cost attributable to providing this service.
				Labor		$ 43.99	Represents the labor cost (e.g. Service Desk, IMAR, platform administration) to support the solution.
A/V Conference Room - Large	Schedule 4.3 - Section 4.13	Install	Fixed Fee Per Unit		$ 64,563.91		
				Hardware		$ 53,588.05	Represents the costs to acquire the Hardware
				Software		$ -	
				Labor		$ 10,975.86	Represents the costs to perform the labor for install and ongoing support
A/V Conference Room - Medium	Schedule 4.3 - Section 4.13	Install	Fixed Fee Per Unit		$ 34,671.93		
				Hardware		$ 28,777.70	Represents the costs to acquire the Hardware
				Software		$ -	
				Labor		$ 5,894.23	Represents the costs to perform the labor for install and ongoing support

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

A/V Conference Room - Small	Schedule 4.3 - Section 4.13	Install	Fixed Fee Per Unit		$ 25,004.76		
				Hardware		$ 20,753.95	Represents the costs to acquire the Hardware
				Software		$ -	
				Labor		$ 4,250.81	Represents the costs to perform the labor for install and ongoing support
Digital Signage Services	Schedule 4.3 - Section 4.14	Subscription	Fixed Monthly Fee Per Unit		$ 73.84		
				Hardware		$ 43.20	Represents the third party costs associated with original configuration and monthly subscription payments for a agreed upon term.
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ -	N/A
				Labor		$ 30.64	Represents costs associated with various with initial installation, help desk, and break/fix labor and support.
Survey Solution Support Services	Schedule 4.3 - Section 4.16	Administrator	Fixed Monthly Fee Per Unit		$ 48.94		
				Hardware		$ -	
				Hardware Maintenance		$ -	
				Software License		$ -	
				Solution support		$ 48.94	Represents costs associated with labor activities to support the solution.
Network Access - Static Wired	Schedule 4.3 - Section 5.5	Device	Fixed Monthly Fee Per Unit		$ 59.74		
				Hardware		$ 16.76	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of a combination of 4 and 5 year refresh cycles.
				Hardware Maintenance		$ 11.83	Represents break-fix services, labor and parts.
				Software		$ 1.97	Represents the costs of software licenses upgrades/refresh. Based on a refresh cycle of 4 years on core network systems and 5 years for edge switches, the aggregated cost is apportioned over the baseline volume of Network Access users.
				Software Maintenance		$ 6.90	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 22.27	Represents labor costs for IMAR activities and circuit costs.
Network Access - Static Wired (Library)	Schedule 4.3 - Section 5.5	Device	Fixed Monthly Fee Per Unit		$ 51.26		
				Hardware		$ 16.16	This component represents the costs of acquiring network assets including switches, routers, security & NAC systems and tools. The component fee is comprised of the monthly amortization of a combination of 4 year refresh cycles for routers and security systems and 5 year refresh cycles for switches.
				Hardware Maintenance		$ 11.41	This component represents break-fix services for hardware assets, primarily labor and parts.
				Software		$ 1.90	This component represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems and 5 years for edge switches, the aggregated cost is apportioned over the baseline volume of Network Access users.
				Software Maintenance		$ 6.66	This component represents costs associated with the labor and resources for Level 2 software support.
				IMAR's		$ 12.01	This component represents labor costs for IMAR activities
				Circuit		$ 3.12	Residual circuits costs
Uninterrupted Power Supply Support Services	Schedule 4.3 - Section 5.5	Device	Fixed Monthly Fee Per Unit		$ 115.50		
				Hardware		$ -	
				Hardware maintenance		$ -	
				Software		$ 86.63	Represents costs associated with monitoring platform
				Software maintenance		$ 25.41	Represents costs associated with maintenance of monitoring platform and labor to support Break/Fix activities

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				IMAR's		$ 3.47	Represents costs associated with IMARs for the addition of new devices for support
Virtual Private Network Access - Level 1	Schedule 4.3 - Section 5.6	Active Account	Fixed Monthly Fee Per Unit		$ 9.88		
				Hardware		$ 2.47	This component represents the costs of acquiring network assets including routers, VPN concentrators, Application Persistence servers, security & NAC systems and tools. The component fee is comprised of the monthly amortization of a combination of 4 year refresh cycles for routers and security systems.
				Hardware Maintenance		$ 1.78	This component represents break-fix services, primarily labor and parts.
				Software		$ 0.38	This component represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems.
				Software Maintenance		$ 1.23	This component represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 1.00	This component represents labor costs for IMAR activities.
				Circuits		$ 3.02	This component represents the cost for intersite bandwidth facilities and Internet access.
Virtual Private Network Access - Level 2	Schedule 4.3 - Section 5.6	Active Account	Fixed Monthly Fee Per Unit		$ 11.46		
				Hardware		$ 1.87	Represents the cost of incremental hardware not included in Infrastructure Services.
				Hardware Maintenance		$ 0.90	Represents break-fix services, primarily labor and parts, not included in Infrastructure Services.
				Software		$ 0.34	Represents the costs of software license acquisition and management.
				Software Maintenance		$ 5.87	Represents software maintenance costs and labor and resources for Level 2 support.
				IMAR's		$ 2.48	Represents labor costs for IMAR activities.
				Circuits		$ -	N/A
Portal - External Users	Schedule 4.3 - Section 5.6	User	Fixed Monthly Fee Per Unit		$ 8.00		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ 4.00	Represents the cost of software license upgrades/refresh.
				Software Maintenance		$ 1.90	Represents costs associated with the labor and resources for Software Maintenance support.
				IMAR		$ 2.10	Represents labor costs for IMAR activities.
Portal - Portfolio Application	Schedule 4.3 - Section 5.6	Application	Fixed Monthly Fee Per Unit		$ 210.90		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ 110.00	Represents the cost of software license upgrades/refresh.
				Software Maintenance		$ 70.90	Represents costs associated with the labor and resources for Software Maintenance support.
				Break Fix		$ 30.00	Represents labor costs for Break Fix activities.
GSMS Short Code Setup	Schedule 4.3 - Section 5.7	Event	Fixed Fee Per Unit		$ 3,885.00		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 3,885.00	Represents the license cost attributable to providing GSMS Short Code Setup.
				Software maintenance		$ -	N/A
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
GSMS Short Code Support	Schedule 4.3 - Section 5.7	Month	Fixed Monthly Fee Per Unit		$ 1,507.63		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ -	N/A

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Software maintenance		$ 1,507.63	Represents the software maintenance cost (e.g. patches, upgrades) attributable to providing GSMS Short Code Support.
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
GSMS Messages	Schedule 4.3 - Section 5.7	Message	Fixed Fee Per Unit		$ 0.03		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 0.03	Represents the license cost attributable to providing GSMS Messages.
				Software maintenance		$ -	N/A
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
IP Conference Phone	Schedule 4.3 - Section 5.7.3	Phone	Fixed Monthly Fee Per Unit		$ 62.70		
				Hardware		$ 29.26	This component represents the costs of Enterprise voice systems comprised of multiple geo-redundant server clusters, IP infrastructure, gateways, IP Conference Phone, and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles.
				Hardware Maintenance		$ 6.93	Represents break-fix services, primarily labor and parts.
				Software		$ 2.31	Represents the costs of software licenses upgrades/refresh based on the refresh cycle of 5 years
				Software Maintenance		$ 2.31	Represents software programming support
				IMAR's		$ 13.60	represents the labor costs for IMAR activities
				Circuits		$ 8.29	Represents the cost for bandwidth and circuitry
Virtual Phone - Microsoft (MS) Teams Phone	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee per Unit		$ 17.69		
				Hardware		$ 2.69	This component represents the costs associated with the hardware required to deploy and operated the AT&T provided Direct Routing solution
				Hardware maintenance		$ 0.27	This component represents break-fix services for enterprise direct routing hardware
				Software		$ 8.78	This component represents cost system and application software, include Microsoft Teams phone license, required to provide direct routing
				Software maintenance		$ 0.20	This component represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 5.75	This component represents labor and support costs for the Direct Routing solution
				Circuits		$ -	
Voice-Avaya Legacy Support	Schedule 4.3 - Section 5.7.3	Month	Fixed Monthly Fee Per Unit		$ 437,522.40		
				Hardware		$ 119,706.67	This component represents enterprise costs of voice system hardware which are fixed
				Hardware maintenance		$ 36,584.63	This component represents break-fix services for enterprise voice hardware
				Software		$ 97,626.38	This component represents the costs of Enterprise voice systems comprised of multiple geo-redundant server clusters, gateways and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles.
				Software maintenance		$ 28,604.12	This component represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 110,360.57	This component represents labor and support costs for Voice Services which are fixed
				Circuits		$ 44,640.05	This component represents the proportion of Voice Services costs of enterprise circuits
Voice Analog Line	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee Per Unit		$ 50.74		

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware		$ 15.99	Represents the costs of Enterprise voice systems comprised of multiple geo-redundant server clusters, analog to IP adapters, gateways and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles.
				Hardware Maintenance		$ 4.74	Represents break-fix services, primarily labor and parts.
				Software		$ 2.37	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of telephones.
				Software Maintenance		$ 2.37	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 20.04	Represents labor costs for IMAR activities.
				Circuits		$ 5.22	Represents the cost for intersite bandwidth facilities and PSTN access.
Voice Single-Line	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee Per Unit		$ 23.98		
				Hardware		$ 7.56	This component represents enterprise costs of voice system hardware which are user volume sensitive. It is comprised of telephone sets and cabling hardware
				Hardware maintenance		$ 2.24	This component represents break-fix services, primarily labor and parts
				Software		$ 1.12	
				Software maintenance		$ 1.12	
				IMAR's		$ 9.47	This component represents labor and support costs for Voice Services which are volume sensitive
				Circuits		$ 2.47	This component represents the proportion of Voice Services costs of enterprise circuits for intersite bandwidth facilities and PSTN access
Voice Multi-Line	Schedule 4.3 - Section 5.7.3	Active Line	Fixed Monthly Fee Per Unit		$ 26.30		
				Hardware		$ 7.44	This component represents enterprise costs of voice system hardware which are user volume sensitive. It is comprised of telephone sets and cabling hardware
				Hardware maintenance		$ 0.90	This component represents break-fix services, primarily labor and parts
				Software		$ -	
				Software maintenance		$ -	
				IMAR's		$ 11.92	This component represents labor and support costs for Voice Services which are volume sensitive
				Circuits		$ 6.05	This component represents the proportion of Voice Services costs of enterprise circuits for intersite bandwidth facilities and PSTN access
Virtual Phone – Microsoft (MS) Teams Phone Advanced Features	Schedule 4.3 Section 5.7.3	Call Flow	Fixed Monthly Fee Per Unit		$ 32.56		
				Hardware		$ -	
				Hardware maintenance		$ -	
				Software		$ -	
				Software maintenance		$ 11.19	Represents costs for maintenance of ACD/AA and monitoring
				IMAR's		$ 21.37	Represents labor costs for IMAR activities
Cloud Access Security Broker	Schedule 4.3 - Section 5.8	Month	Fixed Monthly Fee Per Unit		$ 15,450.12		
				Hardware		$ -	N/A
				Hardware maintenance		$ -	N/A
				Software		$ 14,350.12	Represents the license cost attributable to providing CASB capability
				Software maintenance		$ 1,100.00	Represents the cost associated with the support of the CASB capability
				IMAR's		$ -	N/A
				Circuits		$ -	N/A
Town Hall Services	Schedule 4.3 - Section 5.9	Event	Fixed Fee Per Unit		$ 76,730.20		

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware		$ 13,920.45	12+ VM Servers with Storage Area Network and 4 Video Network Edge appliances (CDN). 5 Year Refresh cycle included.
				Hardware Maintenance		$ 1,962.50	Cloud based and premise based, the 12+ Servers are Cloud based and the VNEs are premise based.
				Software		$ 37,204.55	AVMS/QUMU application license and VNE/CDN licenses. 5 year refresh cycle included.
				Software Maintenance		$ 4,665.43	Application, Content Distribution and Portal support.
				IMAR's		$ 17,045.45	Townhall administrator and Portal updates.
				Circuits		$ 1,931.82	Origination and distribution bandwidth. Originator connectivity limited to available facilities.
Video Conferencing Services - Personal	Schedule 4.3 - Section 5.9	System	Fixed Monthly Fee Per Unit		$ 331.49		
				Hardware		$ 118.36	Represents the costs of VTC roll-about system codec and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 32.18	Represents break-fix services, primarily labor and parts.
				Software		$ 13.85	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for VTC systems, the aggregated cost is apportioned over the baseline volume of VTC end points.
				Software Maintenance		$ 35.64	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 39.38	Represents labor costs for IMAR activities.
				Circuits		$ 92.07	Represents the cost for intersite bandwidth facilities, Internet and PSTN access.
Video Conferencing Services - Room System	Schedule 4.3 - Section 5.9	System	Fixed Monthly Fee Per Unit		$ 955.44		
				Hardware		$ 321.18	Represents the costs of VTC room system codecs and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 102.73	Represents break-fix services, primarily labor and parts.
				Software		$ 39.92	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for VTC systems, the aggregated cost is apportioned over the baseline volume of VTC end points.
				Software Maintenance		$ 102.73	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 113.51	Represents labor costs for IMAR activities.
				Circuits		$ 275.36	Represents the cost for intersite bandwidth facilities, Internet and PSTN access.
Zoom Video Conferencing Support Services	Schedule 4.3 - Section 5.9	Paid Account License	Fixed Monthly Fee Per Unit		$6.95		
				Hardware		$ -	n/a
				Hardware Maintenance		$ -	n/a
				Software		$ -	n/a
				Software Maintenance		$ 4.49	Represents the cost associated with support and maintenance of licenses, including initial assignment, reassignment and true up, break-fix and monthly reporting of free and paid accounts, power and casual users.
				IMAR		$ 2.46	Represents the cost associated with IMAR activities
Video Streaming and Archiving Services	Schedule 4.3 - Section 5.10	System	Fixed Monthly Fee Per Unit		$ 7,283.61		
				Hardware		$ 1,122.22	Represents the switching and router costs of a dedicated VLAN for Video Streaming services and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles for the switch and 4 year refresh cycles for the router.
				Hardware Maintenance		$ 911.44	Represents break-fix services, primarily labor and parts.
				Software		$ 89.71	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for the switch and 4 years for the router, the aggregated cost is apportioned to a single encoder.
				Software Maintenance		$ 911.44	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 1,555.76	Represents labor costs for IMAR activities.
				Circuits		$ 2,693.05	Represents the cost for intersite bandwidth facilities and Internet access.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Video Streaming - COC Chambers	Schedule 4.3 - Section 5.10	System	Fixed Monthly Fee Per Unit		$ 1,282.60		
				Hardware		$ 197.52	Represents the switching and router costs of a dedicated VLAN for Video Streaming services and support the Refresh tasks. The component fee is comprised of the monthly amortization of 5 year refresh cycles for the switch and 4 year refresh cycles for the router.
				Hardware Maintenance		$ 160.33	Represents break-fix services, primarily labor and parts.
				Software		$ 19.24	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for the switch and 4 years for the router, the aggregated cost is apportioned to a single encoder.
				Software Maintenance		$ 159.04	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 275.76	Represents labor costs for IMAR activities.
				Circuits		$ 470.71	Represents the cost for intersite bandwidth facilities and Internet access.
Wireless Access Point	Schedule 4.3 - Section 5.12	Device	Fixed Monthly Fee Per Unit		$ 168.19		
				Hardware		$ 53.82	This component represents the costs of acquiring WiFi access assets including a Wireless Access Point and a proportional amount of redundant controllers/NAC and support the Refresh tasks. The component fee is comprised of the monthly amortization of 3 year refresh cycles.
				Hardware Maintenance		$ 31.95	This component represents break-fix services, primarily labor and parts.
				Software		$ 19.62	This component represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 3 years for WiFi network systems, the aggregated cost is apportioned over the baseline volume of Wireless Access Points.
				Software Maintenance		$ 48.77	This component represents costs associated with the labor and resources for Level 2 support and the County WAN/LAN connectivity.
				IMAR's		$ 14.02	This component represents labor costs for IMAR activities.
Network Access - Wire/Wireless	Schedule 4.3 - Section 5.12	Active Account	Fixed Monthly Fee Per Unit		$ 68.86		
				Hardware		$ 17.52	Represents the costs of acquiring network assets including switches, routers, security & NAC systems and tools. The component fee is comprised of the monthly amortization of a combination of 4 year refresh cycles for routers and security systems and 5 year refresh cycles for switches.
				Hardware Maintenance		$ 13.01	Represents break-fix services, labor and parts.
				Software		$ 3.00	Represents the costs of software licenses upgrades/refresh. Based on a refresh cycle of 4 years on core network systems and 5 years for edge switches, the aggregated cost is apportioned over the baseline volume of Network Access users.
				Software Maintenance		$ 7.00	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 5.75	Represents labor costs for IMAR activities.
				Circuits		$ 22.58	Represents the cost for intersite bandwidth facilities and Internet access.
3rd-Party Network Access - Category 1	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 548.07		
				Hardware		$ 202.53	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 4 year refresh cycles.
				Hardware Maintenance		$ 105.92	Represents break-fix services, labor and parts.
				Software		$ 31.43	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems, the aggregated cost is apportioned over the baseline volume of 3rd Party Network Access users.
				Software Maintenance		$ 133.76	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 74.42	Represents labor costs for IMAR activities.
3rd-Party Network Access - Category 2	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 555.21		
				Hardware		$ 202.30	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 4 year refresh cycles.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware Maintenance		$ 105.80	Represents break-fix services, labor and parts.
				Software		$ 31.39	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems, the aggregated cost is apportioned over the baseline volume of 3rd Party Network Access users.
				Software Maintenance		$ 142.53	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 73.18	Represents labor costs for IMAR activities.
3rd-Party Network Access - Category 3	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 568.32		
				Hardware		$ 206.01	Represents the costs of acquiring network assets and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 4 year refresh cycles.
				Hardware Maintenance		$ 107.74	Represents break-fix services, primarily labor and parts.
				Software		$ 31.97	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 4 years for core network systems, the aggregated cost is apportioned over the baseline volume of 3rd Party Network Access users.
				Software Maintenance		$ 143.29	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 79.31	Represents labor costs for IMAR activities.
3rd Party Network Access - IP Sec - 5 Mbps	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 255.85		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 243.59	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.26	Represents labor costs for IMAR activities.
3rd Party Network Access - IP Sec - 10 Mbps	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 442.39		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 429.62	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.77	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (1 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 153.51		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 141.25	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.26	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (2 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 260.12		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 247.86	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 12.26	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (3 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 340.45		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Software Maintenance		$ 329.45	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 11.00	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (4 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 473.32		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 458.79	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 14.53	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (5 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 609.53		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 595.11	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 14.42	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (6-10 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 1,166.54		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 1,137.82	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 28.72	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (20 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 1,907.15		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 1,850.34	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.81	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (30 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 2,504.79		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 2,447.97	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.82	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (40 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 2,879.77		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 2,822.95	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.82	Represents labor costs for IMAR activities.
3rd Party Network Access - Virtual Access (50 Mbps)	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 3,032.09		
				Hardware		$ -	N/A

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 2,975.27	Represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 56.82	Represents labor costs for IMAR activities.
3rd Party Network Access - Microsoft Teams Rooms	Schedule 4.3 - Section 5.13	Network	Fixed Monthly Fee Per Unit		$ 369.66		
				Hardware			
				Hardware Maintenance			
				Software			
				Software Maintenance		$ 344.15	This component represents costs associated with the labor and resources for Level 2 support and access bandwidth.
				IMAR's		$ 25.51	This component represents labor costs for IMAR activities.
External DNS Management	Schedule 4.3 - Section 5.14	Month	Fixed Monthly Fee Per Unit		$ 15,275.83		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Software Maintenance		$ 12,220.03	Represents costs associated with the labor and resources for Level 2 support and access bandwidth. Also includes the cost of Akamai service.
				IMAR's		$ 3,055.80	Represents labor costs for IMAR activities.
External DNS Management Enhancement	Schedule 4.3 - Section 5.14	Month	Fixed Monthly Fee Per Unit		$ 29,539.27		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software		$ -	N/A
				Platform Support		$ 1,395.14	Monitor Bot Management dashboard and respond to incidents.
				Software Maintenance		$ 26,864.46	Represents costs associated with the labor and resources for Level 2 support related to the Kona Security and Bot Management services.
				IMAR's		$ 1,279.67	Represents labor costs for IMAR activities.
New Site Install - Type I Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 244,519.76		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 244,519.76	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type II Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 122,259.84		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 122,259.84	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type III Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 84,706.98		

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 84,706.98	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type IV Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 71,182.99		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 71,182.99	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type V Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 17,630.81		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 17,630.81	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
New Site Install - Type VI Fixed Component	Schedule 4.3 - Section 5.16	Install	Fixed Fee Per Unit		$ 3,356.91		
				Hardware		$ -	N/A (Network Hardware/systems provided as part of Network Access RUs).
				Software		$ -	N/A (Network Systems software provided as part of Network Access RUs).
				Labor		$ 3,356.91	Represents the labor costs associated with the establishment of New Sites. To include: development of design standards; core circuit order and installation; planning and engineering; installation of Network hardware and software (not including the hardware and software); provisioning and turn up of the New Site, and project management.
Interactive Voice Services - Small	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 721.88		
				Hardware		$ 39.04	Represents the costs of acquiring IP PBX systems that provide Auto Attendant and ACD functions with Contact Management Services and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 143.40	Represents break-fix services, primarily labor and parts.
				Software		$ 78.11	Represents the costs of software licenses upgrades/refresh and programming. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of IVS systems.
				Software Maintenance		$ 233.86	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 92.85	Represents labor costs for IMAR activities.
				Circuits		$ 134.61	Represents the cost for intersite bandwidth facilities and PSTN access.
Interactive Voice Services - Medium	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 2,858.63		
				Hardware		$ 154.59	Represents the costs of acquiring IP PBX systems that provide Auto Attendant and ACD functions with Contact Management Services with Virtual Wall Boards, Automated Call Recording infrastructure and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 567.87	Represents break-fix services, primarily labor and parts.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Software		$ 309.33	Represents the costs of software licenses such as Automatic Call Recording, Virtual Wall Boards and Agent Softphones, upgrades/refresh and programming. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of IVS systems.
				Software Maintenance		$ 926.09	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 367.68	Represents labor costs for IMAR activities.
				Circuits		$ 533.07	Represents the cost for intersite bandwidth facilities and PSTN access.
Interactive Voice Services - Large	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 8,646.33		
				Hardware		$ 467.58	Represents the costs of acquiring IP PBX systems that provide Auto Attendant and ACD functions with Contact Management Services with Wall Boards, Integrated Voice Response (IVR), Computer-Telephony Interface (CTI), Short Message Service (SMS), Work Force Management (WFM) and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 1,717.61	Represents break-fix services, primarily labor and parts.
				Software		$ 935.61	Represents the costs of software licenses including IVR, CTI, SMS and WFM, upgrades/refresh and programming. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of IVS systems.
				Software Maintenance		$ 2,801.09	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 1,112.10	Represents labor costs for IMAR activities.
				Circuits		$ 1,612.33	Represents the cost for intersite bandwidth facilities and PSTN access.
Interactive Voice Services - Support for County Retained	Schedule 4.3 - Section 5.17	System	Fixed Monthly Fee Per Unit		$ 638.68		
				Hardware		$ 44.41	Represents the costs of acquiring PBX trunking hardware and support the Refresh tasks. The component fee is comprised of the monthly depreciation of 5 year refresh cycles.
				Hardware Maintenance		$ 61.58	Represents break-fix services, labor and parts.
				Software		$ 1.18	Represents the costs of software licenses upgrades/refresh. Based on the Refresh Cycle of 5 years for voice based systems, the aggregated cost is apportioned over the baseline volume of County owned IVS systems.
				Software Maintenance		$ 31.97	Represents costs associated with the labor and resources for Level 2 support.
				IMAR's		$ 55.18	Represents labor costs for IMAR activities.
				Circuits		$ 444.36	Represents the cost for intersite bandwidth facilities and PSTN access.
FirstNet Mobility Services	Schedule 4.3 - Section 5.18	Device	Fixed Monthly Fee Per Unit		$ 33.06		
				Support Services		$ 2.16	Includes billing and admin support
				NASPO based carrier plan		$ 30.90	Represents the carrier costs with Taxes and Surcharges included
FirstNet Mobility Services - Tethered	Schedule 4.3 - Section 5.18	Device	Fixed Monthly Fee Per Unit		$ 38.43		
				Support Services		$ 2.16	Includes billing and admin support
				NASPO based carrier plan		$ 36.27	Represents the carrier costs with Taxes and Surcharges included
Mobility Services Hot Spot	Schedule 4.3 - Section 5.18	Device	Fixed monthly fee per unit		$ 26.85		
				Support Services		$ 2.16	Includes billing and admin support
				NASPO based carrier plan		$ 24.69	Represents the carrier costs with Taxes and Surcharges included
Citrix Account	Schedule 4.3 - Section 6	Account	Fixed Monthly Fee Per Unit		$ 20.68		
				Hardware		$ 8.05	Represents the costs of acquiring the asset and support for Refresh tasks. The component fee is the monthly lease payments for a leasing term of 4 years.
				Hardware Maintenance		$ 7.39	Represents break-fix services, primarily labor and parts, including reporting activities.
				Software Licenses		$ 1.55	Represents the cost of software license upgrades/refresh. Based on the Refresh Cycle of 4 years.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Software Maintenance		$ 3.69	Represents costs associated with the labor and resources for Software Maintenance support.
Virtual Guest Server - Cloud IaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Per Unit		$ 534.73		
				Hardware		$ -	N/A
				Operating System License		$ 37.43	Represents the cost of software license upgrades/refresh.
				Other Software License		$ 26.73	Represents an allocation of corporate tools charges.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 470.56	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Cloud PaaS	Schedule 4.3 - Section 6	Server	Fixed Monthly Per Unit		$ 401.05		
				Hardware		$ -	N/A
				Operating System License		$ -	N/A
				Other Software License		$ 20.05	Represents an allocation of corporate tools charges.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 381.00	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Clonetab Solution	Schedule 4.3 - Section 6	Month	Fixed Monthly Per Unit		$ 6,211.24		
				Hardware		$ 263.32	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 18.81	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Storage		$ 5,270.83	Represents the storage costs necessary to implement the solution
				Other Software License		$ 28.21	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 39.50	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 590.58	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
DIMSNET Solution	Schedule 4.3 - Section 6	Month	Fixed Monthly Fee Per Unit		$ 15,369.32		
				Hardware		$ 1,873.96	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 113.76	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Storage		$ 9,681.66	Represents the storage costs necessary to implement the solution
				Other Software License		$ 170.62	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 281.10	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 3,248.22	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
WildFire Scanning Service	Schedule 4.3 - Section 6	Month	Fixed Monthly Fee Per Unit		$ 6,658.80		
				Hardware		$ 510.81	Represents the hardware costs, installation and monthly cost for the duration of the service.
				Hardware Maintenance		$ -	
				Software License		$ 5,223.43	Represents the costs related to the third party software subscription services
				Platform support		$ 924.56	Represents costs associated with monitoring activities and responding to incidents.
NetBackup Solution	Schedule 4.3 - Section 6	Month	Fixed Monthly Fee Per Unit		$ 107,963.65		
				Hardware		$ 86,631.99	Represents the hardware, hardware maintenance and software subscription cost.
				Hardware Maintenance		$ -	
				Software License		$ -	Represents the costs related to the third party software subscription services
				Solution support		$ 21,331.66	Represents costs associated with labor activities to support the solution.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Mainframe	Schedule 4.3 - Section 6.6	CPU Hour***	Fixed Monthly Fee Per Unit		$ 89.87		
				Hardware		$ -	N/A
				Operating System License		$ 18.87	Represents the cost of software license upgrades/refresh. The aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 3.59	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 67.40	Represents costs associated with operating system license maintenance and the labor and resources for Level 2 support.
AS/400	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 2,962.73		
				Hardware		$ -	N/A
				Operating System License		$ -	N/A
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 1,659.13	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 1,303.60	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Copia Fax Line	Schedule 4.3 - Section 6.7	Fax Line	Fixed Monthly Fee Per Unit		$ 125.00		
				Hardware		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software License		$ -	N/A
				Software Maintenance		$ -	N/A
				Circuits		$ 125.00	Represents the cost for intersite bandwidth facilities and PSTN access.
Low Code Application Platform - OutSystems	Schedule 4.3 Section 6.7	User	Fixed Monthly Per Unit		$ 54.06		
				Hardware		$ 8.91	Represents the costs associated to the platform cloud hosting.
				Software License		$ 21.17	Represents the software licenses costs of the platform and users licenses.
				Software Maintenance		$ 11.16	Represents vendor support costs.
				Support Labor		$ 12.82	Represents costs associated with platform support.
Oracle Exadata Services - Eighth Rack	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 10,380.95		
				Hardware		$ 4,159.43	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. Exadata X6-2 Eighth Rack 2 x Exadata Server Nodes (22 cores, 512 GB memory each) 18 x Exadata Storage Nodes (43 TB useable - high redundancy) Bare Metal Install
				Hardware (Refresh Labor)		$ 499.19	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 706.67	Represents the labor costs to support the Oracle Exadata servers ,
				Software License		$ 1,200.00	Represents the software license costs to support the Oracle Exadata servers ,
				Hardware Maintenance		$ 2,495.66	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 1,320.00	Represents costs associated with various software maintenance costs.
Oracle Exadata Services - Backup and Recovery	Schedule 4.3 - Section 6.7	Used Terabyte	Fixed Monthly Fee Per Unit		$ 122.88		
				Hardware		$ 32.81	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Operating System License		$ 2.97	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 9.93	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ 10.81	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 66.36	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Oracle Exadata X8M - Production	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 40,951.09		
				Hardware		$ 8,811.20	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. - Exadata X8M -2 Quarter Rack - 2 x Exadata Server Nodes (48 cores, 1.5 TB memory each) - Each of the 3 High Capacity Storage Cells includes: - 36 x 14 TB disk drives, 1.5 TB of Persistent Memory - 504 TB of raw disk space - 150 TB of usable with High Redundancy ASM storage
				Hardware (Install/Refresh Labor)		$ 274.32	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 1,452.05	Represents the labor costs to support the Oracle Exadata servers.
				Software license		$ 10,962.28	Represents the software license costs to support the Oracle Exadata servers, including Oracle Active Data Guard and Advanced Security.
				Hardware Maintenance & Hosting		$ 7,262.54	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 12,188.70	Represents costs associated with various software maintenance costs, including Oracle Active Data Guard and Advanced Security.
Oracle Exadata X8M - Development / Test	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 33,503.21		
				Hardware		$ 8,811.20	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. - Exadata X8M -2 Quarter Rack - 2 x Exadata Server Nodes (48 cores, 1.5 TB memory each) - Each of the 3 High Capacity Storage Cells includes: - 36 x 14 TB disk drives, 1.5 TB of Persistent Memory - 504 TB of raw disk space - 150 TB of usable with High Redundancy ASM storage
				Hardware (Install/Refresh Labor)		$ 274.32	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 1,452.05	Represents the labor costs to support the Oracle Exadata servers.
				Software license		$ 7,435.62	Represents the software license costs to support the Oracle Exadata servers, including Advanced Security.
				Hardware Maintenance & Hosting		$ 7,262.54	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 8,267.48	Represents costs associated with various software maintenance costs, including Advanced Security.
Oracle Exadata X8M - Business Continuity	Schedule 4.3 - Section 6 .7	Server	Fixed Monthly Fee Per Unit		$ 41,268.64		

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware		$ 9,082.07	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years. - Exadata X6-2 Quarter Rack - 2 x Exadata Server Nodes (48 cores, 1.5 TB memory each) - Each of the 3 High Capacity Storage Cells includes: - 36 x 14 TB disk drives, 1.5 TB of Persistent Memory - 504 TB of raw disk space - 150 TB of usable with High Redundancy ASM storage - Oracle Platinum Gateway Server
				Hardware (Refresh Labor)		$ 292.56	Represents the labor to install and refresh hardware amortized over the estimated asset life. This cost does not include data migration and remediation labor.
				Support Labor		$ 1,452.05	Represents the labor costs to support the Oracle Exadata environment.
				Software License		$ 10,962.28	Represents the software license costs to support the Oracle Exadata servers, including Oracle Active Data Guard and Advanced Security.
				Hardware Maintenance		$ 7,290.97	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 12,188.70	Represents costs associated with various software maintenance costs, including Oracle Active Data Guard and Advanced Security.
Physical Server UNIX - Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 4,537.06		
				Hardware		$ 1,860.20	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 68.06	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 45.37	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 453.70	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 2,109.73	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server UNIX - Medium	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 2,692.34		
				Hardware		$ 1,238.48	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 53.85	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 40.39	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 188.47	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 1,171.16	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server UNIX - Small	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,684.89		
				Hardware		$ 673.96	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 33.70	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 33.70	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 269.58	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 673.95	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server UNIX - X-Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 5,238.56		
				Hardware		$ 2,147.81	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 78.58	Represents the labor to install and refresh hardware amortized over the estimated asset life.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Operating System License		$ -	N/A
				Other Software License		$ 52.39	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 523.85	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 2,435.93	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Unix - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 4,628.27		
				Hardware		$ 1,897.59	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 69.42	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 46.29	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 462.82	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 2,152.14	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,559.37		
				Hardware		$ 545.78	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 31.19	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 46.78	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 81.87	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 853.76	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - Medium	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,085.38		
				Hardware		$ 325.61	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 21.71	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 32.56	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 48.84	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 656.65	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - Small	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 874.58		
				Hardware		$ 244.88	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 17.49	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating System License		$ -	N/A
				Other Software License		$ 26.24	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 36.73	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software Maintenance		$ 549.23	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - X-Large	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,823.60		
				Hardware		$ 796.83	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Hardware (Refresh Labor)		$ 31.19	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 46.78	Represents an allocation of corporate tools charges and anti-virus costs to support servers.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware Maintenance		$ 95.05	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 853.76	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Physical Server Wintel - X-Large - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,732.42		
				Hardware		$ 756.98	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 29.63	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 44.44	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 90.29	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 811.07	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Windows	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 572.95		
				Hardware		$ -	N/A
				Operating System License		$ 40.11	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 28.65	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 504.20	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Windows - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 544.31		
				Hardware		$ -	N/A
				Operating System License		$ 38.10	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 4 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 27.21	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 479.00	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Unix	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,203.20		
				Hardware		$ -	N/A
				Operating System License		$ 84.22	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 36.10	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 1,082.88	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Unix - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 1,143.04		
				Hardware		$ -	N/A
				Operating System License		$ 80.02	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 34.29	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Software Maintenance		$ 1,028.73	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Linux	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 601.60		
				Hardware		$ -	N/A
				Operating System License		$ 42.11	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 30.08	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 529.41	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Guest Server - Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 571.52		
				Hardware		$ -	N/A
				Operating System License		$ 40.01	Represents the cost of software license upgrades/refresh. Based on the physical host refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 28.58	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 502.93	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Host Server - Windows / Linux	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 4,955.61		
				Hardware		$ 2,725.58	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 99.11	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 148.67	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 463.14	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 1,519.10	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Virtual Host Server - Windows / Linux - CWSD Dev/Test	Schedule 4.3 - Section 6.7	Server	Fixed Monthly Fee Per Unit		$ 4,707.83		
				Hardware		$ 2,589.31	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ 94.15	Represents the labor to install and refresh hardware amortized over the estimated asset life.
				Operating system license		$ -	N/A
				Software license		$ 141.24	Represents an allocation of corporate tools charges and anti-virus costs to support servers.
				Hardware Maintenance		$ 439.98	Represents the cost of the Maintenance Agreement for hardware support and break-fix services.
				Software maintenance		$ 1,443.15	Represents costs associated with various software license and maintenance costs, along with the labor and resources for Level 2 support.
Acclaim Riverbed	Schedule 4.3 - Section 6.8	Server	Fixed Monthly Fee Per Unit		$ 1,905.36		
				Hardware		$ 854.43	Represents the hardware costs, architecture, installation and monthly lease payments for a leasing term of 4 years.
				Hardware (Refresh Labor)		$ -	n/a
				Operating System License		$ -	n/a
				Other Software License		$ -	n/a
				Hardware Maintenance		$ 720.93	Represents the third party costs to maintain the hardware.
				Support Labor		$ 330.00	Represents Contractor labor to install and break fix the hardware.
				Software Maintenance		$ -	n/a

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

Infrastructure Services	Schedule 4.3 -- Section 6.8	Month	Fixed Monthly Fee Per Unit		$ 335,063.58		
				Service Desk Services		$ -	N/A
				End User Services		$ 87,381.67	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Infrastructure Services in support of End User Services.
				Network Services		$ 170,804.16	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Infrastructure Services in support of Network Services.
				Data Center Services		$ 76,877.75	Represents the portion of Labor, Hardware, Software and Other Direct Costs to provide Infrastructure Services in support of Data Center Services.
				Application Maintenance & Operations Services		$ -	N/A
				Application Development Services		$ -	N/A
				Hardware			Represents the hardware cost of the Routers, Switches and circuit costs, Servers. Refresh has been included based on depreciation period shown on Exhibit 16.1-1.
				Software			Represents the software costs associated with Infrastructure hardware and Software to run the environment.
				Labor			Represents the Labor to support Infrastructure Services as defined in Section 2.8 of the Technical Proposal.
Development & Test Services	Schedule 4.3 - Section 6.9	Month	Fixed Monthly Fee Per Unit		$ 235,207.11		
				Service Desk Services		$ -	N/A
				End User Services		$ -	N/A
				Network Services		$ -	N/A
				Data Center Services		$ -	N/A
				Application Maintenance & Operations Services		$ 83,171.22	Represents the portion of Dev and Test services attributable to providing Application Maintenance & Operations Services.
				Application Development Services		$ 152,035.89	Represents the portion of Dev and Test services attributable to providing Application Development Services.
				Hardware			Represents the hardware cost of the Routers, Switches and circuit costs, Servers to support the Development and Test environment. Refresh has been included based on depreciation period shown on Exhibit 16.1-1.
				Software			Represents the software costs associated with Development and Test Services Software.
				Labor			Represents the Labor to support Development and Test Environment as defined in Section 2.8 of the Technical Proposal.
Virtual Fax	Schedule 4.3 - Section 6.10	Account	Fixed Monthly Fee Per Unit		$ 38.28		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ -	Represents the cost of software license upgrades/refresh.
				Other Software License		$ 27.05	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 7.03	Represents costs associated with software maintenance along with the labor and resources for support by vendor and Contractor.
				IMAR		$ 4.20	Represents the labor costs for IMAR activities.
Attached Storage – AS/400	Schedule 4.3 -- Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.70		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System license		$ -	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	Represents the estimate of the Non-OS License Software

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware maintenance		$ 0.185	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software maintenance		$ 0.510	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Attached Storage – Mainframe	Schedule 4.3 -- Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 6.73		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System license		$ -	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	Represents the estimate of the Non-OS License Software
				Hardware maintenance		$ 2.09	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software maintenance		$ 4.64	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Attached Storage - Unix	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.73		
				Hardware		$ 0.23	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ -	N/A
				Other Software License		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 0.50	Represents costs associated with storage management software, and the labor and resources for Level 2 support.
Attached Storage - WINTEL	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.52		
				Hardware		$ 0.19	Represents the hardware costs, installation and monthly lease payments for a leasing term of 4 years.
				Operating System License		$ -	N/A
				Other Software License		$ -	N/A
				Hardware Maintenance		$ -	N/A
				Software Maintenance		$ 0.33	Represents costs associated with storage management software, and the labor and resources for Level 2 support.
Storage - Archive Tier	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.20		
				Hardware		$ 0.11	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 0.01	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 0.02	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 0.05	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 0.02	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Primary Tier	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.47		
				Hardware		$ 0.12	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 0.01	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 0.04	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 0.04	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 0.26	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Secondary Tier	Schedule 4.3 - Section 6.12	Used Gigabyte	Fixed Monthly Fee Per Unit		$ 0.32		
				Hardware		$ 0.08	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Operating System License		$ 0.01	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 0.03	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 0.03	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 0.17	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Document Processing Center 1	Schedule 4.3 - Section 6.12	Unit	Fixed Monthly Fee Per Unit		$ 17,408.16		
				Hardware		$ 9,032.90	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years
				Operating System License		$ 1,733.08	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 974.86	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 3,617.03	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 2,050.29	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Document Processing Center 2	Schedule 4.3 - Section 6.12	Unit	Fixed Monthly Fee Per Unit		$ 10,319.40		
				Hardware		$ 5,354.62	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years
				Operating System License		$ 1,027.35	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 577.89	Represents the estimate of the Non-OS License Software in support of the DPC.
				Hardware Maintenance		$ 2,144.14	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 1,215.40	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Immutable Tier (1TB)	Schedule 4.3 - Section 6.12	1 Terabyte	Fixed Monthly Fee Per Unit		$ 355.57		
				Hardware		$ 177.43	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 100.63	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 27.38	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 50.14	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
Storage - Immutable Tier (500GB)	Schedule 4.3 - Section 6.12	512 Gigabyte	Fixed Monthly Fee Per Unit		$ 177.79		
				Hardware		$ 88.54	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ 50.14	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ -	N/A
				Hardware Maintenance		$ 13.69	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 25.42	Represents costs associated with software maintenance along with the labor and resources for Level 2 support.
NetBackup Solution Amazon Web Services	Schedule 4.3 - Section 6.13	TB	Fixed Monthly		$ 86.31		
				Hardware		$ -	NA
				Hardware Maintenance		$ -	NA
				Software License		$ 53.82	Represents the costs related to the third party software subscription services

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Solution Support		$ 32.49	Represents costs associated with labor activities to support the solution.
Enterprise Application Access	Schedule 4.3 - Section 2.6	Month	Fixed Monthly Fee Per Unit		$ 78,203.57		
				Hardware		$ -	Represents the hardware costs, installation and monthly lease payments for a leasing term of 5 years.
				Operating System License		$ -	Represents the cost of software license upgrades/refresh. Based on the refresh cycle of 5 years, the aggregated cost is apportioned over the assumed baseline volumes.
				Other Software License		$ 56,218.59	Represents the estimate of the Non-OS License Software.
				Hardware Maintenance		$ -	Represents the cost of the Maintenance Agreement for hardware support and break-fix services, for the hardware noted above.
				Software Maintenance		$ 21,984.98	Represents costs associated with software maintenance along with the labor and resources for support by vendor and Contractor.
Optional Item Catalog (OIC) - Software Addition	Exhibit 16.1 - Section 10.2	Add	Fixed Fee Per Unit		$ 2,450.00		
				Hardware		$ 221.32	Represents the lab workstations used to test MSI packing.
				Operating System License		$ -	
				Other Software License		$ 48.28	Represents desktop software packaging and installation kit software.
				Hardware Maintenance		$ -	
				Software Maintenance		$ 2,180.40	Represents the labor costs for adding software to the catalog of available software.
Optional Item Catalog (OIC) - Update	Exhibit 16.1 - Section 10.2	Update	Fixed Fee Per Unit		$ 1,470.00		
				Hardware		$ 118.19	Represents the lab workstations used to test MSI packing.
				Operating System License		$ -	
				Other Software License		$ 27.46	Represents desktop software packaging and installation kit software.
				Hardware Maintenance		$ -	
				Software Maintenance		$ 1,324.35	Represents the labor costs for updating software to the catalog of available software.
Transition Services - Service Desk Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit				
				Hardware			N/A
				Software			N/A
				Labor			N/A
Transition Services - Application Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit				
				Hardware			N/A
				Software			N/A
				Labor			N/A
Transition Services - End User Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit				
				Hardware			N/A
				Software			N/A
				Labor			N/A
Transition Services - Network Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit				
				Hardware			N/A
				Software			N/A
				Labor			N/A
Transition Services - Data Center Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit				

Exhibit 16.1-6a Resource Unit Price Decomposition Option Term

				Hardware			N/A
				Software			N/A
				Labor			N/A
Transition Services - Cross Functional Services Framework	Schedule 2.1	Milestone	Fixed Fee Per Unit				
				Hardware			N/A
				Software			N/A
				Labor			N/A
Transition Services - Transition Completion	Schedule 2.1	Milestone	Fixed Fee Per Unit				
				Hardware			N/A
				Software			N/A
				Labor			See TS7 - Completion tab for details.

*Schedule 4.3 Reference includes the Section reference for the specific requirements for this particular Resource Unit but it still includes all general requirements applicable to such Resource Unit in the higher levels of the obligations hierarchy as described in Schedule 4.3. For example, the Resource Unit for Desktop - Standard Workstation includes not only the responsibilities as stated in Section 4.5 of the End-User Services Section of Schedule 4.3, but also the responsibilities in Sections 4.1 through 4.3 of the End-User Services Section, as well as the responsibilities and requirements in Section 1 of Schedule 4.3.

**The mainframe RU unit volumes are based on the R24 CPUs

***With the exception of 2.3.1.4 and 2.3.1.5 and their respective requirements

Exhibit 16.1-7 – ELA Pricing Adjustments

1. OVERVIEW

County licenses various software and services from Microsoft Corporation through an Enterprise Agreement ("MSEA"), including but not limited to, Microsoft Office. Contractor, as County's IT outsourcing provider, uses the license to provide Microsoft Office and other software services to County. Contractor is obligated to pay for a portion of the MSEA as part of its right to use the MSEA to provide services to the County and receives remuneration for that cost through various resource units. The MSEA also entitles County, and Contractor as County's outsourcer, to use Microsoft OneDrive and Microsoft 365. The MSEA provides that Microsoft OneDrive and Microsoft 365 are provided at no additional charge. Microsoft OneDrive is provided with no limitation on the amount of storage available to County. County and Contractor anticipate moving a portion of the County storage and Microsoft Office services to Microsoft OneDrive and Microsoft 365 during the Term. County and Contractor acknowledge that Microsoft may, at some point, change the terms of the MSEA to add a charge for Microsoft OneDrive and Microsoft 365, or to limit the storage provided at no charge for Microsoft OneDrive. Similarly, County and Contractor acknowledge that Contractor has provided County with a fixed-price resource unit fee during the Term that includes a projected pricing increase in the MSEA. Based upon the foregoing, County and Contractor agree that, at the beginning of Contract Year 5, County and Contractor will jointly review the cost of the MSEA for the portion of the MSEA Contractor uses to provide the Services to County. If, at that time, Microsoft has added a fee for Microsoft OneDrive or Microsoft 365 or both, or added a charge to meet the County's requirements for OneDrive storage, then based on the new MSEA fees paid for by Contractor (i.e., "Revised Price"), County and Contractor shall adjust the Exhibit 16.1-1 resource units identified in bundle B1 as follows:

1.1 If the Revised Price exceeds the Office 365 Plan "G3" subscription per user per year price of $142.80 plus the Enterprise CAL Office 365 Bridge CAL per user per year price of $24.55 ("Base Price"), Contractor shall be entitled to increase the Exhibit 16.1-1 resource units identified in bundle B1 in an amount equal to the difference between the Base Price and the Revised Price.

1.2 If the Revised Price is less than the Base Price, Contractor shall reduce the Exhibit 16.1-1 resource units identified in bundle B1 in an amount equal to the difference between the Base Price and the Revised Price.

END OF EXHIBIT

Schedule 16.7 — Benchmarking Methodology

Table of Contents

1. Benchmarking Company 3
2. Definition of Benchmark 3
3. Benchmarking Costs 4
4. Benchmarking Procedures 4
5. General Agreement of Cooperation 5
6. Benchmarking Metrics 5
7. Peer Comparison and Benchmark Performance Requirements 6

1. BENCHMARKING COMPANY

The benchmarking program will be conducted by an independent industry-recognized benchmarking service ("Benchmarking Company") designated by County and the parties will jointly validate the proposed firm's capabilities and fit with the requirements of this Schedule 16.7 Contractor shall not unreasonably withhold approval of the proposed firm. The following firms shall be pre-approved as candidates to carry out the benchmarking program: PricewaterhouseCoopers, LLP, Alsbridge, Inc., and any other Benchmarking Company agreed to in writing by the CIO and Account Executive. The Benchmarking Company shall: (i) be independent, (ii) have demonstrable experience in performing information technology benchmarks ("Benchmark"), and (iii) agree to maintain the confidentiality of all data. Neither Party shall unreasonably delay the signing of such an agreement.

2. DEFINITION OF BENCHMARK

With County's direction, and as a part of the Services, the Benchmarking Company shall conduct a benchmarking program that shall enable County to compare the Fees and Service Levels (SLs) set forth in this Agreement with, and to ensure that said Fees and SLs are among, the industry's competitive rates and SLs for such Services, Frameworks or Framework Components.

The Benchmarking Company will "normalize" all data to obtain relevant comparisons for purposes of the Benchmark. Factors related to general normalization to be taken into consideration by the Benchmarking Company may include, but shall not be limited to: (i) geographic location of the peer companies; (ii) industry differences affecting information technology costs; (iii) economies of scale; (iv) workload and complexity factors (including operating environment).

In addition, factors related to normalization for outsourced services may include, but shall not be limited to: (i) the SLs offered; (ii) duration and nature of the contractual commitment; (iii) volume of services being provided; (iv) contractual terms, conditions and allocation of risk; (v) amount of investment made by Contractor in the customer's equipment and personnel; (vi) appropriate overhead; and (vii) provisions to ensure the unique factors of each deal are taken into account by the Benchmarking Company and appropriate adjustments will be made for out-of-scope deliverables, however method of delivery is not a unique factor unless Contractor is contractually obligated to County for a unique delivery requirement.

3. BENCHMARKING COSTS

The Parties will (i) share equally the costs and expenses of conducting the Benchmarking and (ii) jointly enter into a written agreement with the Benchmarking Company.

4. BENCHMARKING PROCEDURES

County may request a benchmark for (i) Services, (ii) Frameworks, (iii) a part of any individual Framework to be comprised of at least thirty percent (30%) of the number of Framework Components (two-thirds of which will be selected by County one-third of which will be selected by Contractor) comprising any Framework, or (iv) Service Level at any time after the first year of the Term, provided that a benchmark cannot be undertaken more than one time in any 12-month period. Upon designation of the benchmark timing, a non-retroactive date will be set by both parties that any necessary pricing changes will be in effect; provided that such date shall not be later than 60 days after the start of the benchmarking process, unless otherwise agreed by the parties. In addition, the Parties shall meet with the Benchmarking Company for the purpose of agreeing upon a detailed plan (including time deadlines for provision of data by Contractor) for implementing the Benchmark.

Contractor agrees that should it fail to provide data or otherwise comply in a timely manner in accordance with the agreed plan, Contractor shall have a grace period of fourteen (14) days in which to provide such data or compliance, after which County's monthly invoice from Contractor for Services shall be reduced by 1%, of the average of the previous 12 monthly invoices, for each day of such failure by Contractor. If the failure exceeds 90 days, such failure shall be deemed an Event of Default at the County's sole discretion, and County may terminate the Agreement or relevant Framework(s).

Within fifteen (15) days of the Benchmark Notice Date County and Contractor will meet to jointly review the Benchmark results. If the report of the Benchmarking Company concludes that the then-current Contractor's aggregate Fees for an IT Framework(s) or selected part of any individual Framework selected by County is greater than 110% of the Benchmarking Company's market-based aggregate fees for such Framework(s) or selected part of any individual Framework selected by County, then either: Option 1 (i) Within 30 days after the Benchmarking Company provides its report to the Parties, Contractor shall notify County in writing if Contractor has elected to accept the determination of the Benchmarking Company, and, if Contractor so elects to accept such determination, Contractor shall promptly reduce the applicable Fees to not more than 105% of such market-based aggregate fees; or Option 2 (ii) If benchmarking (a) discloses material variations between Contractor's charges and/or quality standards, and prevailing market standards, within 30 days after the Benchmarking Company provides its report to

the Parties, Contractor shall notify County in writing if Contractor intends to dispute the determination of the Benchmarking Company, (b) Contractor shall promptly reduce the applicable Fees to not more than 105% of such market-based aggregate, and (c) the parties shall engage in good-faith negotiations to determine an appropriate rate, and (d) if the parties are unable to negotiate an appropriate rate, Contractor may utilize the Dispute Resolution process set forth in Section 23 of the Agreement to dispute the benchmarking process and/or benchmarking results.

In addition, if any SLs are lower than the applicable service levels contained in the Benchmark results, with respect to the corresponding Fees, then at County's option, Contractor shall either increase the SLs to match the applicable service levels contained in the Benchmark results, or reduce its Fees proportionately as set forth above to adjust for the difference between the SLs and the applicable service levels contained in the Benchmark results.

5. GENERAL AGREEMENT OF COOPERATION

The Parties acknowledge that the Benchmark definition and procedure described in this Schedule will require further definition and clarification as the Parties begin actual implementation of the Benchmark. The Parties shall cooperate with the utmost good faith to reach reasonable and timely agreements on such further definition and clarification. To the extent that the Benchmarking Company reasonably establishes that certain definitions, procedures and methodologies are widely used in information technology benchmarking, the Parties agree to generally rely on the Benchmarking Company's definitions, procedures and methodologies for guidance in reaching agreement. Furthermore, the Parties acknowledge that in reaching the final results of the Benchmark, the Benchmarking Company will be required to exercise its professional judgment and discretion in certain matters and, assuming such judgments are within established industry practices for information technology benchmarking, the Parties will defer to the conclusions of the Benchmarking Company.

Contractor acknowledges that County views the Benchmark procedure described in this Schedule as a critical inducement to County's agreement to many of the terms of this Agreement, including the Term and termination rights provided for in the Agreement, and therefore Contractor agrees that it will cooperate in good faith to accomplish the objectives of the Benchmark procedure for the benefit of County.

6. BENCHMARKING METRICS

Prior to the commencement of all benchmarking studies, County and Contractor will agree on the specific Services, Frameworks or Framework Components (metrics) to be included within the scope of the study. Also, Contractor will be apprised of the metrics sufficiently in advance of the benchmarking study to establish administrative

processes to capture the necessary metric data. The exact metrics to be included in the benchmark study will be contingent upon: (1) the detail in which the Benchmark Company maintains cost and pricing data within its database; and, (2) Contractor's ability to capture pricing information at the desired level of detail.

7. PEER COMPARISON AND BENCHMARK PERFORMANCE REQUIREMENTS

The Contractor must perform to a level as depicted in the outcome of the Benchmark. The level is the average price point of the peer group.

END OF SCHEDULE

Schedule 16.8 — Fee Reductions

Table of Contents

1. Critical Milestones....3
1.1. Creation and Funding of Critical Milestone Fund....3
1.2. Critical Milestone Process....3
2. Fee Reductions For Service Levels....4
2.1. Service Levels....4
2.2. Calculating Fee Reductions....4
2.3. Several Failures....4
2.4. Cap....5
2.5. Credit of Fee Reductions....5
2.6. Multiple SL Failures....5
2.7. Potential for Earnback....5
2.8. Earnback of SL Related Fee Reductions....6
2.9. Changes to Weighting Factors....8
2.10. Low Volume Condition....8

1. CRITICAL MILESTONES

1.1. Creation and Funding of Critical Milestone Fund

Commencing on the Effective Date, each month during the Term and any period of Disentanglement, the Contractor may only invoice the County ninety percent (90%) of the Monthly Services Charges otherwise payable. The portion of such Monthly Services Charges not invoiced for each six-month period following the Effective Date is referred to herein as the "Six-Month Milestone Fund" and shall be used for the Critical Milestones described in Section 1.2. Fee Reductions for Failure to meet Transition Critical Milestones are not subject to this Section 1.

1.2. Critical Milestone Process

The County in its sole discretion may designate (in accordance with Section 4.12 of the Agreement) one or more milestones as "Critical Milestones," each of which shall consist of certain Services that the County reasonably deems important for Contractor to perform within a six-month period. The County will designate these milestones no later than May 15th each Contract Year for a performance period from July 1 through December 31st, and November 15th of each Contract Year for a performance period from January 1 through June 30th. The County will assign a certain percentage of the Milestone Account to each such Critical Milestone. If the total percentages of the assignments do not total one hundred (100%) of the Six-Month Milestone Fund for a particular period, the County will release the unassigned portions to the Contractor upon Contractor's submission of a proper invoice to County.

Critical Milestones serve as a quality assurance function for the County. The purpose of Critical Milestones is to provide a means to incentivize Contractor performance on Services that are already being performed, or are already committed, for the upcoming 6-month period, including operational services and/or projects. Critical Milestones will not require performance at Service Levels above and beyond what is currently in the Agreement, and will not require performance beyond what is already covered by the Fees, including Resource Units. The County anticipates that Critical Milestones in the initial Contract Years will be focused on Transformation Services; and in the latter Contract Years of the Agreement, on preparation for Transition Services. Prior to establishing any Critical Milestones, the County agrees to discuss with Contractor any potential Critical Milestones and related questions. This obligation does not in any way limit the County's ability to establish Critical Milestones in its sole discretion.

2. FEE REDUCTIONS FOR SERVICE LEVELS

This section describes the methodologies associated with measurement of and reporting on the results achieved in respect to the Service Levels (SL).

2.1. Service Levels

Each SL set forth in this document identifies key performance measures that will be used to evaluate Contractor's delivery of the requested Services. The objective of SLs is to monitor and measure the Contractor's performance on the County's most-important business requirements and; continuous improvement in the Contractor's provision of the Service. New SLs may be added to reflect changing or new business requirements. SLs may be reviewed no less than annually, where appropriate, to adjust the SLs to reflect such continuous improvement in Contractor's provision of the Service. In no event, unless mutually agreed, will the Service Levels or the Fee Reductions set forth herein be reduced below the levels at which they are set on the Effective Date.

2.2. Calculating Fee Reductions

For each Failure relating to a SL, Contractor shall pay or credit to the County a Fee Reduction that will be computed by multiplying (a) Weighting Factor for such SL by (b) SL At Risk Amount. For example, assume for purposes of illustration only, that Contractor has a Failure with respect to a SL with a Weighting Factor of 8% and that the Monthly Service Fees equal $100,000 and the SL At Risk Amount is 10%. The Fee Reduction due to the County for such Failure would be: 8% * (10% * $100,000) = $800.

The "SL At Risk Amount" for any month during the Term is ten percent (10%) of the Monthly Service Fees excluding any fees for Transition as set forth in Schedule 16.1.

The "SL At Risk Pool" is two hundred percent (200%) and is the total percentage points that is be allocated across SLs.

The "Weighting Factor" for any particular SL is the portion of the SL At Risk Pool used to calculate the Fee Reduction payable to the County in the event of a Failure with respect to that SL.

2.3. Several Failures

If more than one Failure with respect to SLs has occurred in a single month, the sum of the corresponding Fee Reductions shall be credited or paid to the County.

2.4. Cap

In no event shall the aggregate amount of Fee Reductions credited or paid to the County with respect to all Failures with respect to SLs occurring in a single month exceed the SL At Risk Amount.

2.5. Credit of Fee Reductions

Contractor shall itemize the total amount of Fee Reductions it is obligated to pay or credit to the County with respect to SL Failures occurring in a given month on the invoice that contains charges for such month. Contractor shall credit the total amount of such Fee Reductions related to a given month on the invoice that contains charges for such month. Upon termination or expiration of the Term, Contractor shall pay to the County the amount of any Fee Reductions not so credited to the County's account or any unused portion of such Fee Reductions.

2.6. Multiple SL Failures

If a Failure with respect to a given SL recurs in consecutive Measurement Periods, the amount of the applicable Fee Reduction payable to the County shall be multiplied by the following factors for subsequent Measurement Periods: (i) SL Failure in two consecutive Measurement Periods, then 1.5 times the amount of the Fee Reduction as originally calculated; and (ii) SL Failure in three or more consecutive Measurement Periods, then twice the amount of the Fee Reduction as originally calculated. The Fee Reduction for any given SL shall only be increased as described above, and such increase shall be payable for all successive consecutive Failures with respect to such SL.

2.7. Potential for Earnback

Following any Failure to meet certain SLs, the Contractor will have an opportunity in future periods of performance of such SL to earn back portions of Fee Reductions provided to the County as a result of such Failure(s) in accordance with the procedures set forth below. During Transition, the County and Contractor shall collaborate in good faith to assign earn back performance levels ("Earn Back Performance Levels") for certain SLs that the County identifies as desirable to receive improvements in performance above and beyond the minimum acceptable level, and to establish for each such SL a number of months that such Earn Back Performance Levels must be met immediately following such Failure to earn back a percentage of a Fee Reduction assessed for such Failure, which percentage shall also be mutually agreed to by the Parties. In the event the County and Contractor are unable to reach written agreement by a date not later than thirty (30) days before the Cutover of each of the Service Frameworks on (i) the SLs for that Service Framework that will be subject to Earn Back Performance Levels, (ii) the actual establishment of such Earn Back Performance Levels, or (iii) the percentage of the

previously assessed Fee Reduction that can be earned back for each such SL, then such implementing details may be established by the County in writing. The Parties acknowledge and agree that not all SLs shall be subject to earn back.

2.8. Earnback of SL Related Fee Reductions

Contractor may earn back a portion of a SL-related Fee Reduction for overachievement of a previously failed SL in the following and successive months. Contractor's earnback of SL-related Fee Reductions shall be subject to the following conditions:

2.8.1. During the time until the Transaction Response Time SL has been implemented, Contractor's SL-related Fee Reduction earn back amount shall be no greater than fifty percent (50%) of the applicable SL-related Fee Reduction.

2.8.2. With the implementation of the Transaction Response Time SL, Contractor's SL-related Fee Reduction earn back amount shall be no greater than seventy five percent (75%) of the applicable SL-related Fee Reduction. Should the County determine not to implement the Transaction Response Time SL, starting the month following that determination, the earn back shall increase from the 50% level to the 75% level.

2.8.3. Earn back will apply on a SL-by-SL basis. Fee Reductions for an earlier failed SL cannot be earned back by overachievement on a different SL.

2.8.4. Contractor shall earn back the allowed portion of a SL-related Fee Reduction by achieving in the immediately successive month(s), a higher SL level than the SL level required for that SL in the Agreement. At the 75% earn back level upon successful completion of the heightened SL requirement as set forth below, Contractor will earn back twenty-five percent (25%) of the appropriate SL-related Fee Reduction for each month within a three month window that Contractor achieves the overachievement threshold for the SL. At the 50% earn back level upon successful completion of the heightened SL requirement as set forth below, Contractor will earn back twenty-five percent (25%) of the appropriate SL-related Fee Reduction for each month within a two month window that Contractor achieves the overachievement threshold for the SL. Contractor may earn back no greater than seventy-five percent (75%) of the applicable SL-related Fee Reduction.

2.8.5. If a month, or months, occurs during the earn back period after a SL failure in which there is no data to calculate SL performance, for the previously failed SL, due to lack of data, then the earn back window for the over-achievement earn back will be extended by the number of months without a SL calculation (i.e., provided that there are no subsequent SL failures, for the SL in question, during the period).

2.8.6. The SL level required for earn back shall be the midpoint between the then-applicable SL level and one hundred percent (100%), or zero percent (0%) for those SLs where the lowest percentage would define perfection. For purposes of clarity and as an example, if Contractor fails to achieve a SL for which the minimum SL level is ninety percent (90%), then to earn back a Fee Reduction for that SL, Contractor's earn back SL level would be ninety-five percent (95%).

2.8.7. Contractor may only earn back SL-related Fee Reductions for applicable SLs within the earn back period following a SL Fee Reduction. For purposes of clarity and as an example, at the 75% earn back level if Contractor incurs a SL-related Fee Reduction in October, Contractor may earn back 25% for each month during the period November, December, and January for which the applicable over achievement SL level was achieved. Each of the three months is considered an independent event. If there is no data to calculate an SL for December, the time period would be extended to February. If Contractor fails to achieve the heightened SL in any month during the earn back period, then Contractor would not receive the 25% earn back for the months in which the heightened performance was not achieved. Therefore, continuing with the foregoing example, if Contractor achieves the heightened SL level in November but fails to achieve the heightened SL level in December, Contractor would receive twenty-five percent (25%) of the SL-related Fee Reduction for the November SL achievement, but would not receive the twenty-five percent (25%) available for December. However, if the Contractor achieved the heightened earn back again in January, the 25% earnback would apply. The Contactor would have realized 50% of the related Fee Reduction over the three-month period in the above example. The Contractor may earn 25% of the related Fee Reduction for each of the next three months after a SL failure for all months the Contractor meets or exceeds the over achievement threshold up to a total of 75% of the related Fee Reduction . If the base SL threshold is missed again during the earn back period, then the earn back period for the base SL is terminated, and the cycle of earnbacks starts again in the next month.

2.8.8. Contractor's earn back of SL-related Fee Reductions is conditioned upon Contractor providing to County timely and auditable data supporting Contractor's achievement of the heightened SL level.

2.9. Changes to Weighting Factors

No more than once every three (3) months during the Term, the County may make changes to the Weighting Factor for any SL by sending written notice (which notice may contain changes to multiple SLs) to Contractor at least thirty (30) days prior to the date that such new percentages are to be effective. With respect to the addition of SLs the County shall modify the Weighting Factors for the SLs such that the sum of the Weighting Factors for all SLs does not exceed the SL At Risk Pool.

2.10. Low Volume Condition

2.10.1. Single Failure Results in Measurement Failing

A low volume condition exists where a single failure of an event-based measurement results in the measurement failing. The intent is to address the inadvertent creation of a perfection measurement when perfection is not the committed target.

For those SLs where there is insufficient volume in one Measurement Period such that a single Performance Target miss would cause SL Failure, that volume will be carried forward and accumulated for the next Measurement Period(s) volume on a rolling basis for that SL, until sufficient volume exists to allow for at least a single Performance Target miss without triggering SL Failure. Once that volume is reached, the SL is measured based on the accumulated volume and reported in the Measurement Period in which sufficient volume was reached. As assurance that low volume does not sacrifice SL performance, more than one failed Performance Target miss in the same Measurement Period, or in multiple Periods before the sufficient volume is reached, triggers SL Failure.

Example 1: Seven (7) out of the eight (8) incidents resolved in January resulted in an SL performance of 87.5% (7 ÷ 8) against a target of 90%. However, since the single missed incident would cause the SL Failure, the volume rolls to February and there is no Fee Reduction in January. The two (2) incidents resolved in February met the target. The accumulated volume for February is 10 (8 from January + 2 from February) which is sufficient volume to allow for a single missed incident without triggering SL Failure (9 ÷ 10 = 90%). The SL performance for February is 90% (9 ÷ 10), which meets the target. The accumulated volume resets for March.

Example 2: Six (6) out of the eight (8) incidents resolved in January resulted in a SL performance of 75% (6 ÷ 8) against a target of 90%. Since there are two failed incidents prior to reaching sufficient volume, SL Failure applies in January and Fee Reduction is applied. The accumulated volume is reset for February.

Example 3: Seven (7) out of the eight (8) incidents resolved in January resulted in an SL performance of 87.5% (7 ÷ 8) against a target of 90%. However, since a single missed incident would cause the SL Failure, the volume rolls to February and there is no Fee Reduction in January. The one (1) incident resolved February did not meet the target. The accumulated volume for February is 9 (8 from January + 1 February), which is still insufficient volume to allow for a single missed incident without triggering SL Failure (8 ÷ 9 = 89%). However, since there are two failed incidents prior to reaching sufficient volume, SL Failure applies in February and a Fee Reduction is applied. The accumulated volume resets for March.

2.10.2. Volume Insufficient to Meet Threshold to Measure SL Performance

A low volume condition exists where the volume doesn't meet the defined threshold to calculate SL performance. The intent is to address the inadvertent creation of an unmeasurable SL due to low volume.

For those SLs where there is insufficient volume in one Measurement Period such that the SL performance cannot be calculated, that volume will be carried forward and accumulated for the next Measurement Period(s) volume on a rolling basis for that SL, until sufficient volume exists to allow for calculation. Once that volume is reached, SL performance is measured based on the accumulated volume and reported in the Measurement Period in which sufficient volume was reached.

Example 1: 200 customer satisfaction survey responses were returned in January, which is less than the defined threshold is 378 for calculation of SL performance. The January volume rolls to February and there is no Fee Reduction. 200 customer satisfaction survey responses were returned in February for an accumulated total of 400 (200 from January + 200 from February), which is sufficient to calculate SL performance. The SL performance for February is 90% (360 survey responses with rating of 3 or 4 ÷ 400 survey responses), which meets the target. The accumulated volume is reset the subsequent month.

Example 2: 200 customer satisfaction survey responses were returned in January, which is less than the defined threshold is 378 for calculation of SL performance. The January volume rolls to February and there is no Fee Reduction. 200 customer satisfaction survey responses were returned in February for an accumulated total of 400 (200 from January + 200 from February), which is sufficient to calculate SL performance The SL performance for February is 80% (320 survey responses with rating of 3 or 4 ÷ 400 survey responses), which fails to meet the target of 90%. SL Failure applies in February and a Fee Reduction is applied. The accumulated volume is reset the subsequent month.

2.10.3. With regard to Multiple SL Failures, only those Measurement Periods in which sufficient volumes are reached will be considered as Consecutive Month(s). For example, if previous month resulted in SL Failure the current month results in a roll over due to low volume, and then the next month results in SL Failure, the next month is considered the Consecutive Month for Multiple SL Failures.

2.10.4. With regard to Earnback of SL Related Fee Reduction, the earn back window for the over-achievement earn back will be extended by the number of months without an SL calculation due to low volume.

END OF SCHEDULE

Schedule 18.2 — Third-Party Contracts

Table of Contents

1. Overview 3

2. List of Third-Party Contracts.....5

1. OVERVIEW

This Schedule 18.2 lists Third-Party contracts into which Contractor enters or of which Contractor accepts assignment and that are subject to the limitation of liability set forth in Section 18.2(e) of the Agreement. This list may be updated from time-to-time by written agreement of County and Contractor, which must be signed by the County CIO and the Contractor's Account Executive. For purposes of clarity, any Third-Party contract not listed on this Schedule 18.2 shall be subject to the terms of the Agreement, including Section 18.2 and shall not be subject to the limitation of liability table set forth in Section 18.2(e).

Only those agreements between Contractor and Third-Parties satisfying one of the following requirements may be added to this Schedule 18.2.

1. Agreements entered into by the County and assigned to Contractor and for which Contractor does not receive remuneration from the County through a resource unit set forth in Schedule 16.1, except that payment of the Third Party Negotiation – Large or Third Party Negotiation – Small Resource Unit shall not independently prevent the inclusion of the Third-Party Contract in this Schedule 18.2.

2. Agreements entered into by Contractor at County's direction, that are not part of a master agreement maintained by Contractor, and for which Contractor does not receive remuneration from the County through a resource unit set forth in Schedule 16.1, except that payment of the Third Party Negotiation - Large or Third Party Negotiation – Small Resource Unit shall not independently prevent the inclusion of the Third-Party Contract in this Schedule 18.2.

The following examples are illustrative of the foregoing:

Example 1 – County Assigned Contract

County enters into an agreement for automobile parts tracking and inventory software for its auto mechanics. That software is loaded into the Contractor data center and the license is assigned by County to Contractor. That license would be added to this Schedule 18.2 and would be subject to the liability limitations set forth in Section 18.2(e).

Example 2 – Contractor Acquired Contract

County requests that Contractor obtain specific software for County for automobile parts tracking and inventory for County's auto mechanics. Contractor obtains that software and loads it into Contractor's data

center. That license would be added to this Schedule 18.2 and would be subject to the liability limitations set forth in Section 18.2(e).

Example 3 – Contractor Acquired Contract

Contractor purchases additional Hardware or Software to support Third-Party Software assigned by County or Third-Party Software acquired by Contractor at County direction (e.g. additional servers or OS licenses). The additional Hardware and Software contracts would not be added to this Schedule 18.2 and would be subject to the general liability provisions of Section 18.2.

Example 4 – Contractor Acquired Contract

Contractor contracts for additional Help Desk Services to comply with the Help Desk requirements of Schedule 4.3. That contract would not be added to this Schedule 18.2 and would be subject to the general liability provisions of Section 18.2.

Example 5 – Contractor Acquired Contract

County requests a new service – virtualized desktops – which require a new resource unit. Contractor obtains Contractor selected and County approved Hardware, Software and other Services required to provide that service. Those contracts would not be added to this Schedule 18.2 and would be subject to the general liability provisions of Section 18.2.

Example 6 – Contractor Acquired Contracts

Contractor contracts for application development services using the application development procedures in Schedule 4.3 or through the application development process set for the Section 7.3 of Appendix 4.3 – Application Development Services. That contract would not be added to this Schedule 4.3 and would be subject to the general liability provisions of Section 18.2.

Example 7 – Enterprise Agreements

County obtains a license from Microsoft for the use of Microsoft products. That license provides that Contractor may use the Microsoft products on Contractor's Hardware and to provide Services to County. That license would not be added to Schedule 18.2 and would be subject to the general liability provisions of Section 18.2.

2. LIST OF THIRD-PARTY CONTRACTS

The list of Third-Party Contracts is published as Schedule 5 Report 167 - Third-Party Contracts for Schedule 18.2.

END OF SCHEDULE

Schedule 19 — Insurance

Table of Contents

1. Insurance 3

1.1. Minimum Scope of Insurance 3

1.2. Minimum Limits of Insurance 3

1.3. Other Insurance Provisions 5

1.4. General Insurance Provisions 5

1. INSURANCE

Without limiting Contractor's indemnification obligations to County, Contractor shall provide at its sole expense and maintain for the duration of this Agreement, or as may be further required herein, insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the Services or Work hereunder and the results of the Services or Work by the Contractor, his agents, representatives, employees or Subcontractors.

1.1. Minimum Scope of Insurance

Coverage shall be at least as broad as:

1.1.1. Commercial General Liability, Occurrence form, Insurance Services Office form CG0001.

1.1.2. Automobile Liability covering all owned, non-owned, hired auto Insurance Services Office form CA0001.

1.1.3. Workers' Compensation, as required by State of California and Employer's Liability Insurance.

1.1.4. Technology Errors and Omissions Liability (including Cyber Security Liability)

1.1.5. Fidelity coverage providing Employee Dishonesty, Forgery or Alteration, Theft, Disappearance, Destruction and Computer Fraud coverage covering all Contractor's employees.

1.1.6. Property Insurance.

1.2. Minimum Limits of Insurance

Contractor shall maintain the following limits:

1.2.1. Commercial General Liability including Premises, Operations, Products and Completed Operations, Contractual Liability, and Independent Contractors Liability: $5,000,000 per occurrence for bodily injury, personal injury and property damage. The Project Specific Aggregate limit shall be $10,000,000.

1.2.2. Automobile Liability: $1,000,000 each accident for bodily injury and property damage.

1.2.3. Workers' Compensation as required by any applicable law or regulation having jurisdiction over Contractor's employees. Employer's Liability: $1,000,000 each accident for bodily injury or disease. Coverage shall include a waiver of subrogation endorsement in favor of County of San Diego.

1.2.4. Technology Errors and Omissions Liability (including Cyber Security Liability): $10,000,000 per claim with an aggregate limit of not less than $20,000,000. The County may request annually that Contractor confirm if any self-retained limit is greater than $500,000 and if it is greater, shall disclose that amount to the County. The coverage will not contain specific, express exclusions for design errors, destruction of data or failure to designing an adequate system arising out of Contractor's wrongful acts in the rendering of, or failure to render, professional technical services to the County. This coverage shall be maintained for a minimum of two years following termination or completion of Contractor's Services pursuant to the Agreement. Cyber Security Liability under this policy includes Privacy Liability (unauthorized disclosure by the Contractor of private information or failure to protect private information that results in identity theft) and Failure of Security (inability of the security of the Contractor's computer system to mitigate loss from or prevent a computer attack or physical theft of hardware, theft of password or access code).

1.2.5. Comprehensive Crime Insurance, Employee Dishonesty and Computer Fraud: $10,000,000 per occurrence. Such insurance shall cover all of Contractor's employees. Coverage shall include a loss payee endorsement to the County. Any deductible or self-insured retention shall be the responsibility of Contractor.

1.2.6. Property Insurance: Contractor shall provide insurance on all property owned by Contractor and provided under this Agreement. Such policy shall provide "all risk" perils, and shall be written on a basis of one hundred percent (100%) replacement value of the property. Coverage shall include business personal property, tenant improvements, business interruption, property of others, in the care, custody, and control of the insured, and transit. Any deductible or self-insured retention shall be the responsibility of Contractor.

1.3. Other Insurance Provisions

The general liability and automobile liability are to contain, or be endorsed to contain the following provisions:

1.3.1. Additional Insured Endorsement (Does not apply to Technology Errors and Omissions Liability 1.2.4.)

Any general and automobile liability policy provided by Contractor shall contain an additional insured endorsement applying coverage to the County of San Diego, the members of the Board of Supervisors of the County and the officers, agents, employees and volunteers of the County, individually and collectively. This requirement may be met through the use of a blanket additional insured endorsement.

1.3.2. Primary Insurance Endorsement

For any claims related to this Agreement, the Contractor's insurance coverage shall be primary insurance as respects the County, the members of the Board of Supervisors of the County and the officers, agents, employees and volunteers of the County, individually and collectively. Any insurance or self-insurance maintained by the County, its officers, officials, employees, or volunteers shall be excess of the Contractor's insurance and shall not contribute with it.

1.3.3. Notice of Cancellation.

Notice of Cancellation shall be in accordance with policy provisions.

1.3.4. Severability of Interest Clause.

Coverage applies separately to each insured, except with respect to the limits of liability, and that an act or omission by one of the named insureds shall not reduce or avoid coverage to the other named insureds.

1.4. General Insurance Provisions

1.4.1. Qualifying Insurers

With the exception of any wholly owned captive all required policies of insurance shall be issued by companies which have been approved to do business in the State of California by the State Department of Insurance, and which hold a current policy holder's alphabetic and financial size category rating of not less than A-, VII according to the current Best's Key Rating guide, or a company of equal financial

stability that is approved in writing by County Risk Management. Such approval shall not be unreasonably withheld.

1.4.2. Evidence of Insurance

Prior to commencement of this Agreement, but in no event later than the Effective Date of the Agreement, Contractor shall furnish the County with certificates of insurance and amendatory endorsements effecting coverage required by this clause. Renewal certificates and required amendatory endorsements effecting coverage shall be furnished to County within thirty (30) days of the expiration of the term of any required policy. Contractor shall, upon request, provide the County with a summary of its insurance policies.

1.4.3. Failure to Obtain or Maintain Insurance; County's Remedies

Contractor's failure to provide insurance specified or failure to furnish certificates of insurance and amendatory endorsements or failure to make premium payments required by such insurance, shall constitute a material breach of the Agreement, and County may, at its option, terminate the Agreement for any such default by Contractor provided that the same is not cured within thirty (30) days of Contractor's receipt of notice from the County specifying the nature of the claimed default.

1.4.4. No Limitation of Obligations

The foregoing insurance requirements as to the types and limits of insurance coverage to be maintained by Contractor, and any approval of said insurance by the County are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by Contractor pursuant to the Agreement, including, but not limited to, the provisions concerning indemnification.

1.4.5. Review of Coverage

County retains the right at any time to review the coverage, form and amount of insurance required herein and may request Contractor to obtain insurance reasonably sufficient in coverage, form and amount to provide adequate protection against the kind and extent of risk which exists at the time a change in insurance is required.

1.4.6. Self-Insurance

With the exception of Workers' Compensation, Contractor may, with the prior written consent of County Risk Management, fulfill some or all of the insurance requirements

contained in this Contract under a plan of self-insurance. Contractor shall only be permitted to utilize such self-insurance if in the opinion of County Risk Management, Contractor's (i) net worth, and (ii) reserves for payment of claims of liability against Contractor, are sufficient to adequately compensate for the lack of other insurance coverage required by this Contract. Contractor's utilization of self-insurance shall not in any way limit liabilities assumed by Contractor under the Contract.

1.4.7. Claims Made Coverage

If coverage is written on a "claims made" basis, the Certificate of Insurance shall clearly so state. In addition to the coverage requirements specified above, such policy shall provide that:

(i) The policy retroactive date coincides with or precedes Contractor's commencement of Services under the Agreement (including subsequent policies purchased as renewals or replacements);

(ii) Contractor will make every effort to maintain similar insurance during the required extended period of coverage following expiration of the Agreement, including the requirement of adding all additional insureds;

(iii) If insurance is terminated for any reason, Contractor shall purchase an extended reporting provision of at least two years to report claims arising in connection with the Agreement; and

(iv) The policy allows for reporting of circumstances or incidents that might give rise to future claims.

1.4.8. Subcontractors' Insurance

Contractor shall require that any and all Subcontractors hired by Contractor are insured in accordance with this Contract. If any Subcontractors coverage does not comply with the foregoing provisions, Contractor shall defend and indemnify the County from any damage, loss, cost or expense, including attorney fees, incurred by County as a result of Subcontractors' failure to maintain required coverage.

1.4.9. Waiver of Subrogation

Contractor and County release each other, and their respective authorized representatives, from any Losses (as defined in Section 22.1 of the Agreement), but only to the extent that the proceeds received from any policy of insurance carried by County or Contractor, other than any self-insurance, covers any such Losses. With the exception of Technology Errors and Omissions Liability insurance and Crime Insurance, included in any policy or policies of insurance provided by Contractor hereunder shall be a standard waiver of rights of subrogation against County by the insurance company issuing said policy or policies.

END OF SCHEDULE