

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.

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.

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

Application Services Achievement

HPES achieved a 100% rating on all Priority-1-under-4-hours application service calls.

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.

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.

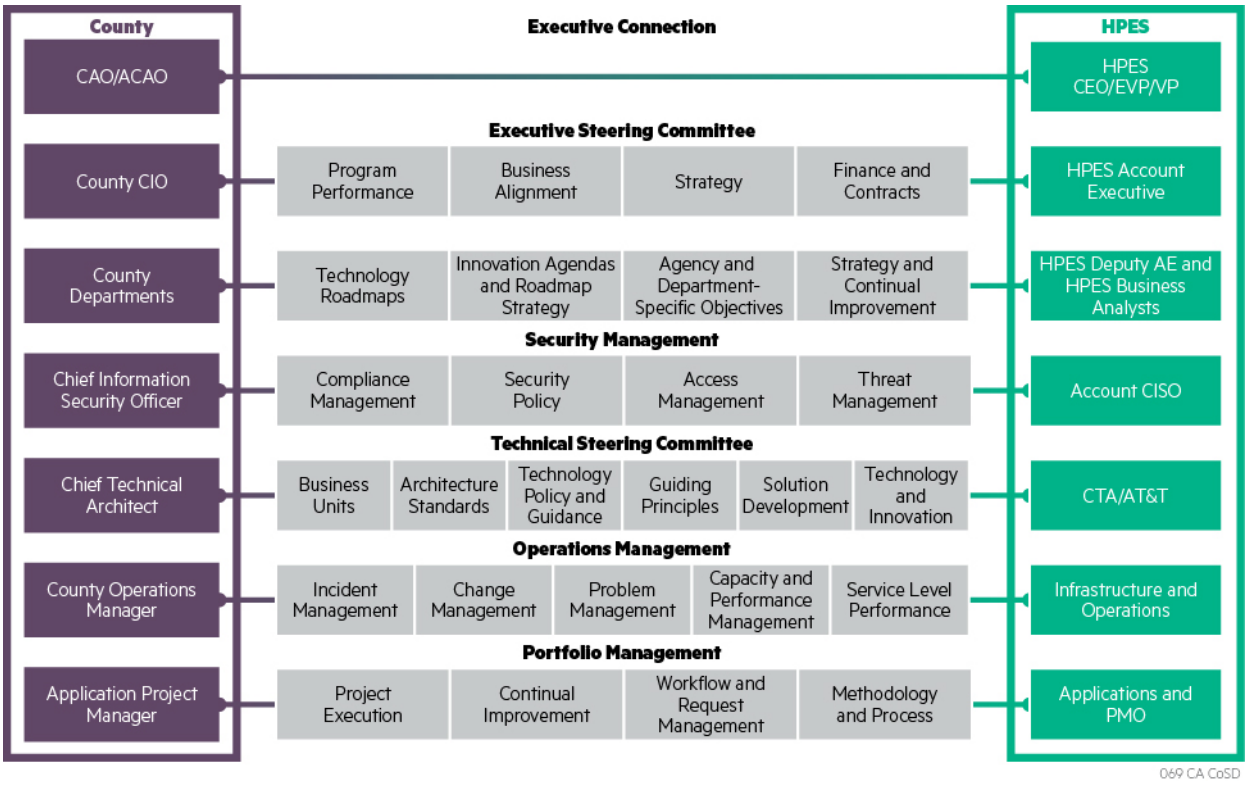
Service Framework 5 – Application Services. HPES supports approximately 100 applications for the City. The applications range in size from small MS Access applications to large enterprise class applications, such as Enterprise Resource Planning (ERP) and Customer Information System (CIS). EnQuesta—which 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.

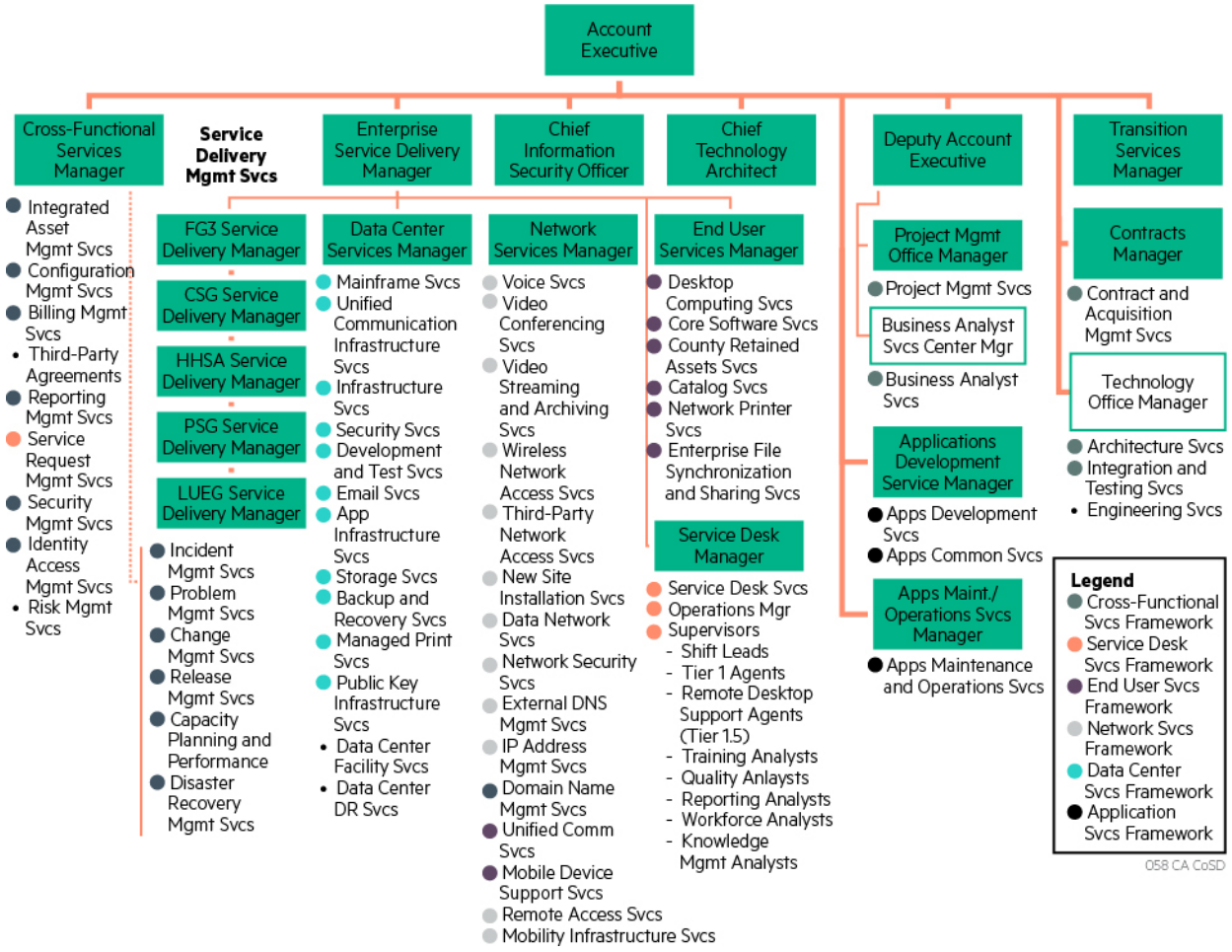
High-caliber, experienced team ready Day One = Continuity of resources for lowest-risk transition

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.

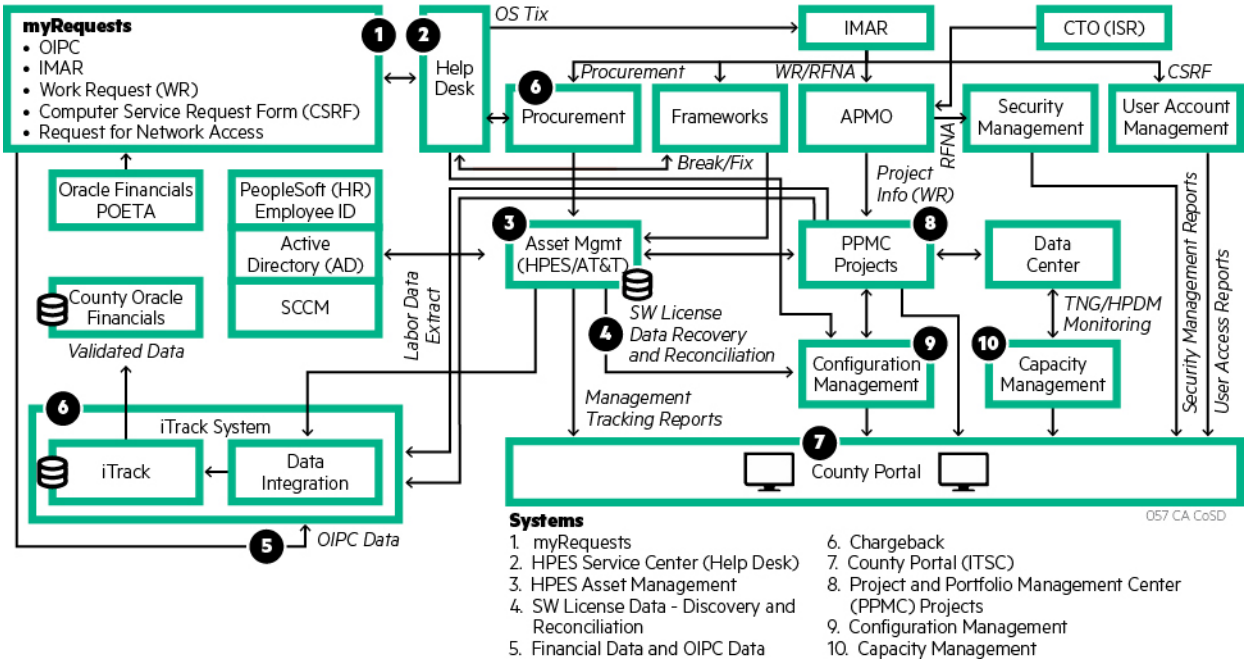
2.5 Cross-Functional Services Framework

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.

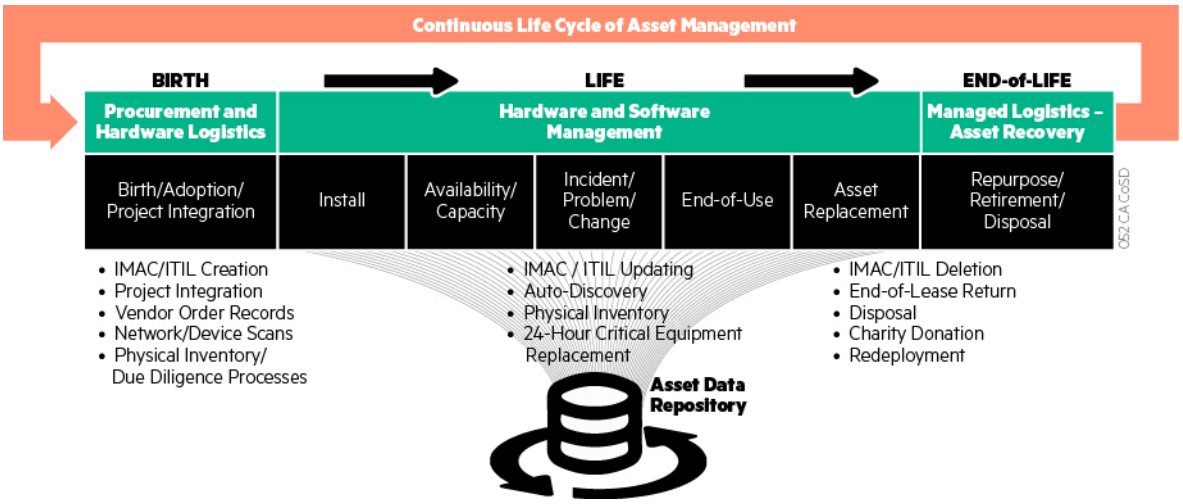
The IT asset manager and warehouse lead will operate from the HPES Rancho Bernardo facility. HPES will also leverage resources located at our Tulsa data center—the asset management team will process assets into Asset Manager and provide site support technicians based out of the Rancho Bernardo facility 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.

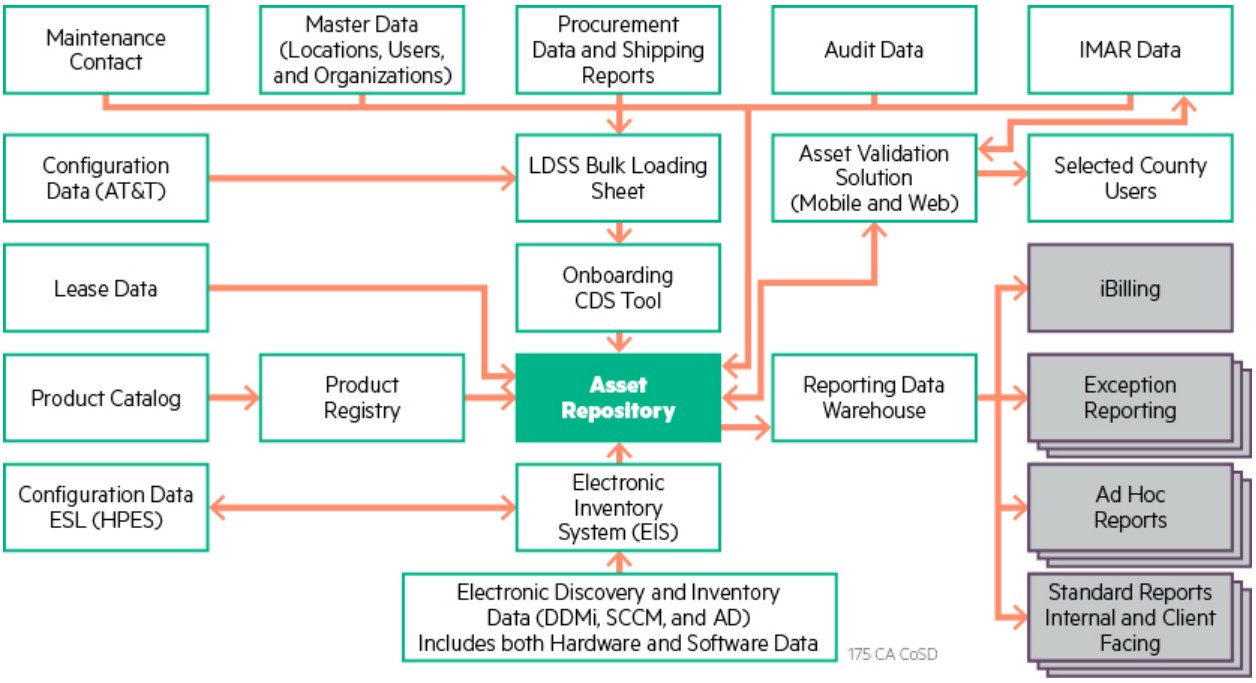
Asset Retirement/Charitable Donation

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.

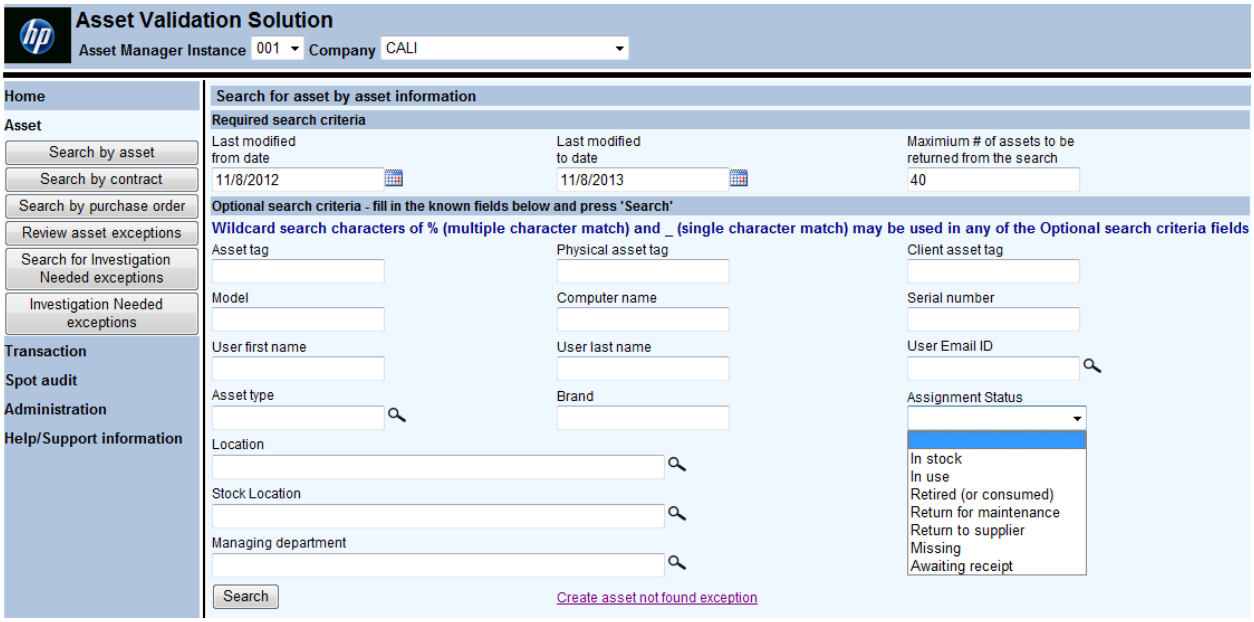
Figure 5 shows the Integrated Asset Management systems, data sources, and their integrations.

- **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.

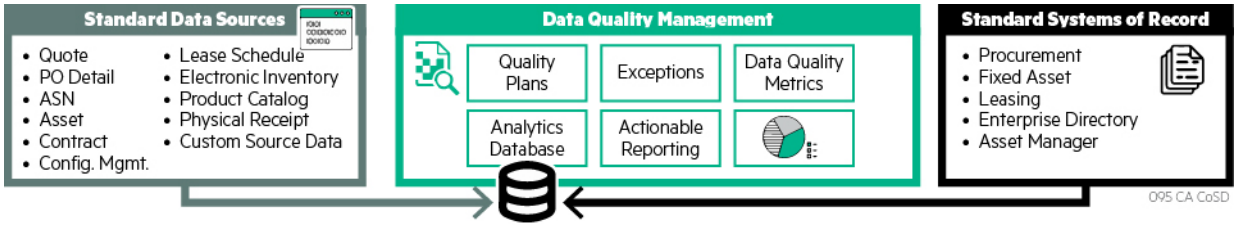
All changes to CI's are managed through our ITIL-based change management process. No changes to assets will be allowed unless previously approved.

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

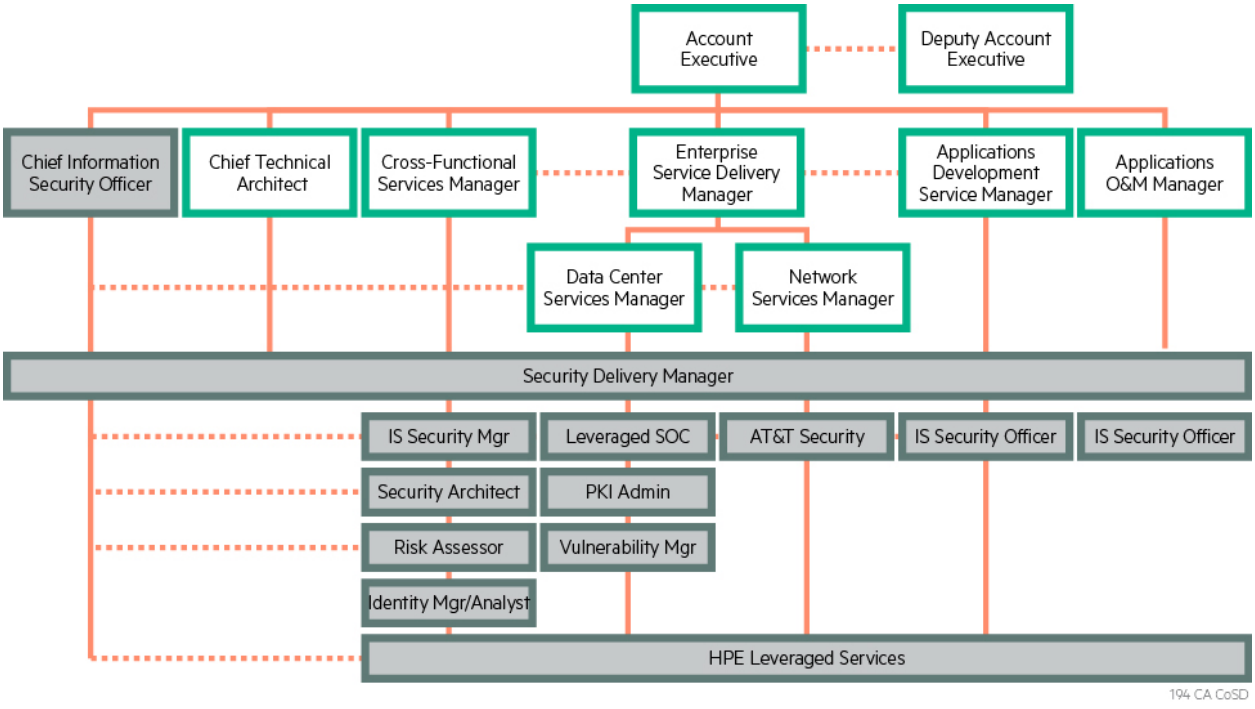
Solution: HPES' approach to security management adheres to the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) and its Special Publication 800 series, which will act as a guide for delivery and compliance for the protection of systems and providing security 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

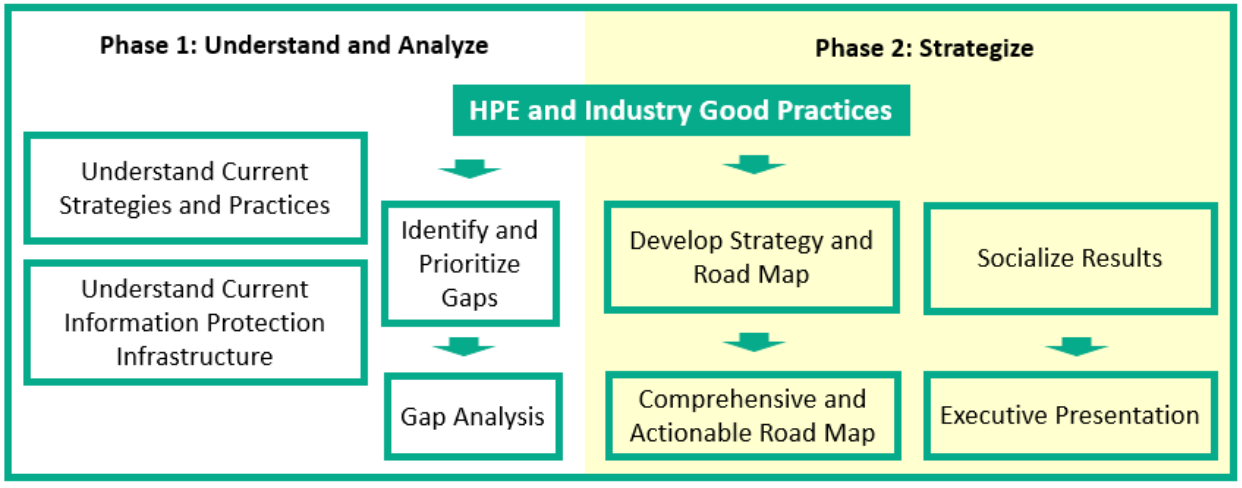
third-party vendors. As more hybrid cloud-based solutions are introduced to solve business needs, the controls surrounding third-party vendors will be rigorously tested and enhanced to minimizes risk and avoid delays. Controls designed to monitor ingress and egress of data, data flows, audit and accountability, 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.

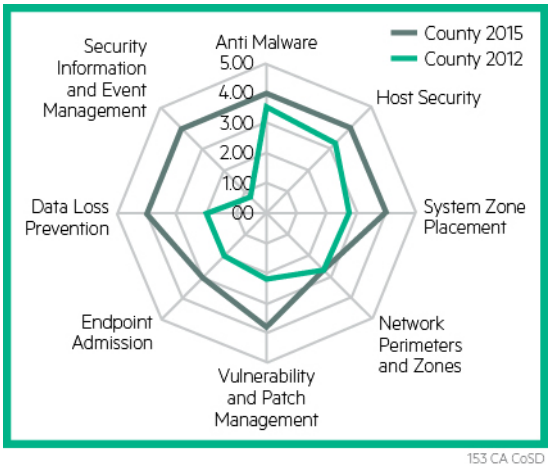
- **Endpoint Admission:** What approaches the County uses to control client endpoint admission to zones and resources.
- **Host Security:** What management and protection postures the County takes with regard to host system security.
- **Vulnerability and Patch Management:** How the County manages and 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.

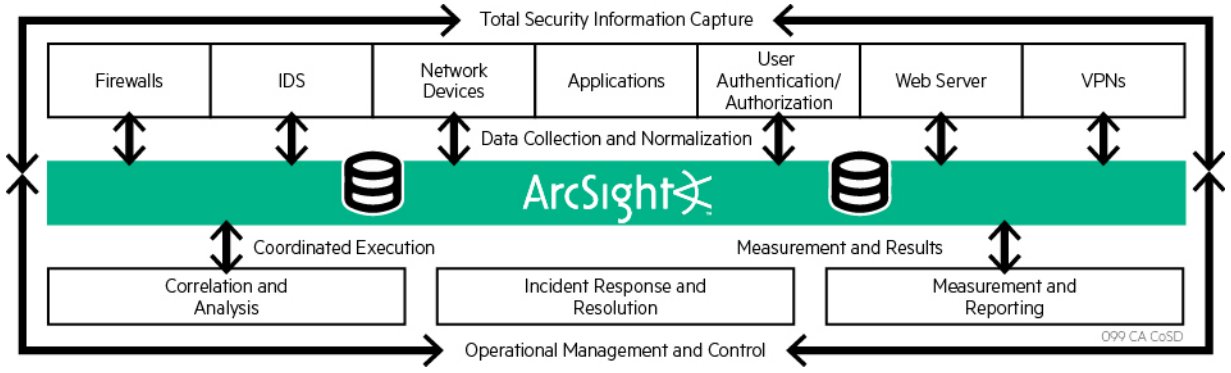
2.5.4.2. Describe your proposed approach to data analysis of SIEM information and remediation of identified risks or vulnerabilities.

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.

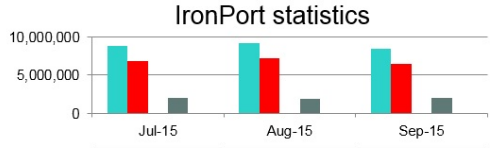
2.5.4.3. Describe your proposed approach to assess the County's security environment.

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

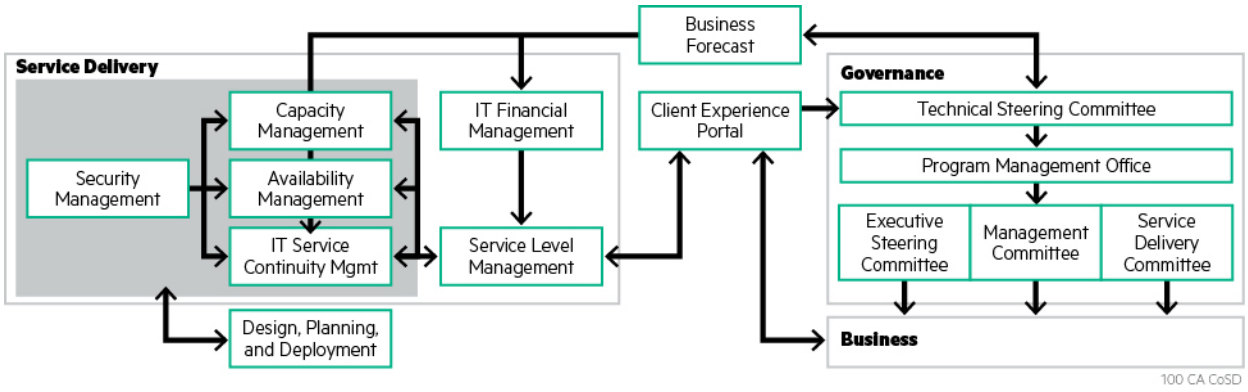
The SDMs are required to have face-to-face interaction with their business groups in addition to email, phone, etc.

- 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.

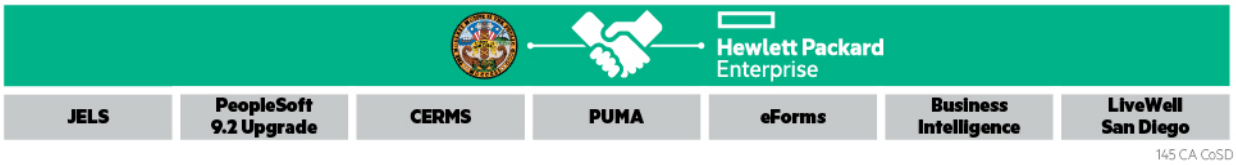
2.5.6 (Reserved)

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:

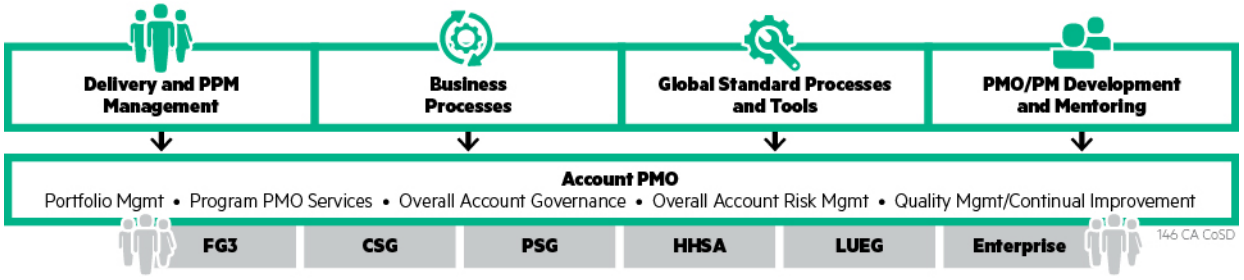
- Identify and use global best practices as a framework for creating tailored, relatable, and customer-centric procedures that provide the best fit to meet our customers' evolving needs, while driving quality and expedience into our delivery model.
- Provide frequent, accurate updates to the County Project 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

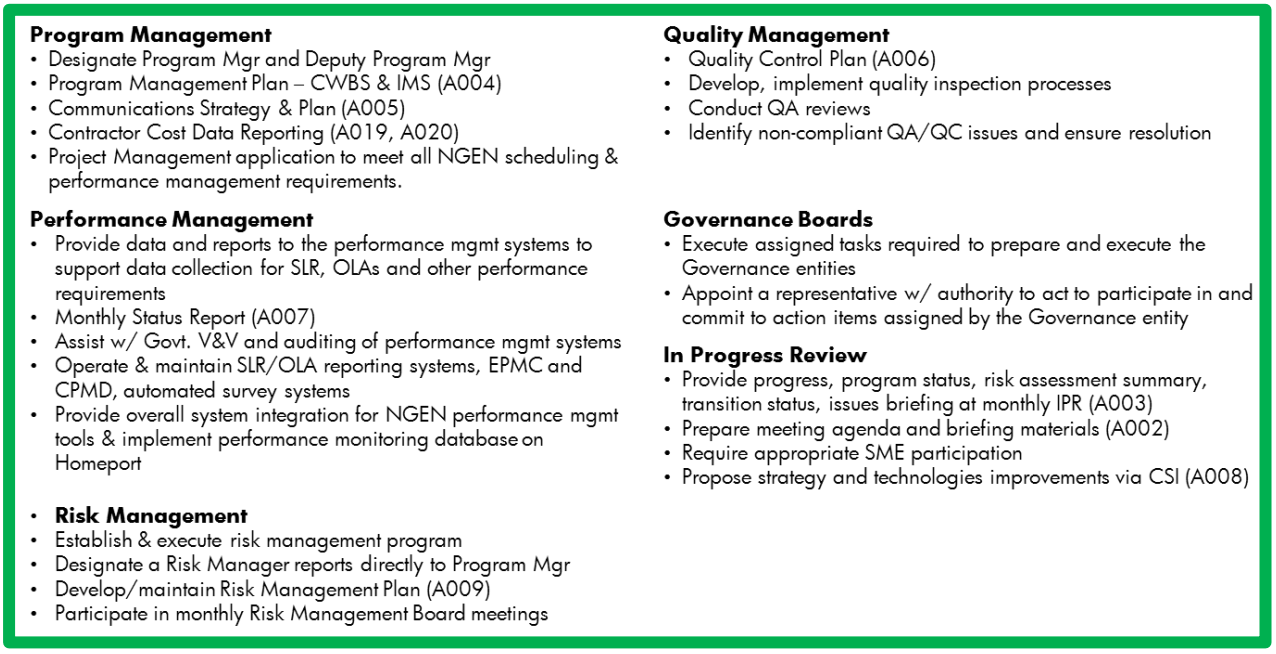
With more than 10 years of successful project management for the County, our combined teams have developed a quality base to build upon for our next generation agreement. Since 2012, our team has completed more than 5,000 project initiatives for the County. From large, enterprise work requests to small, 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.

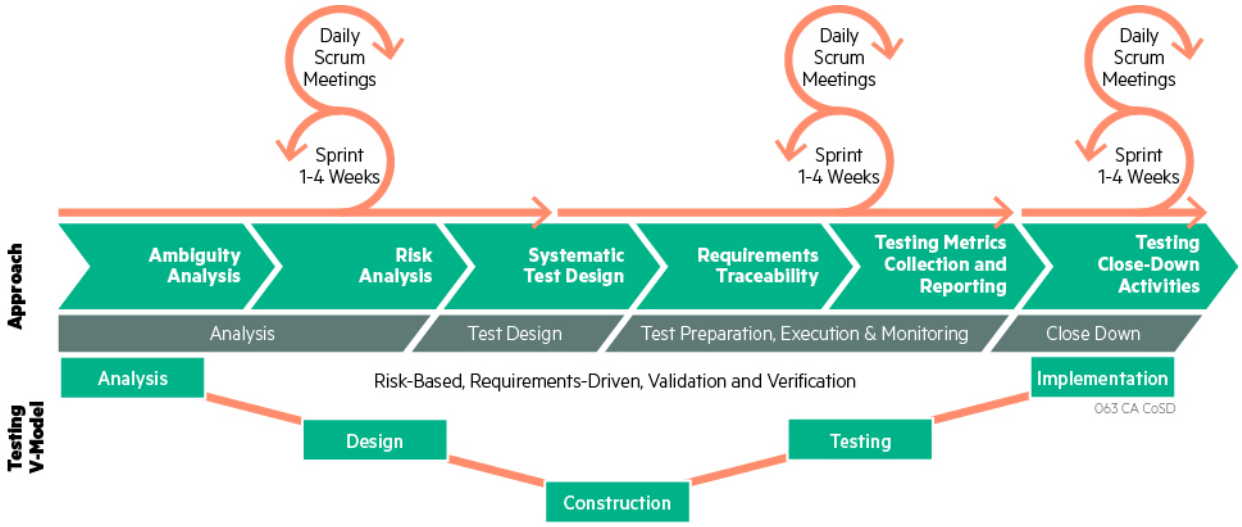
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

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

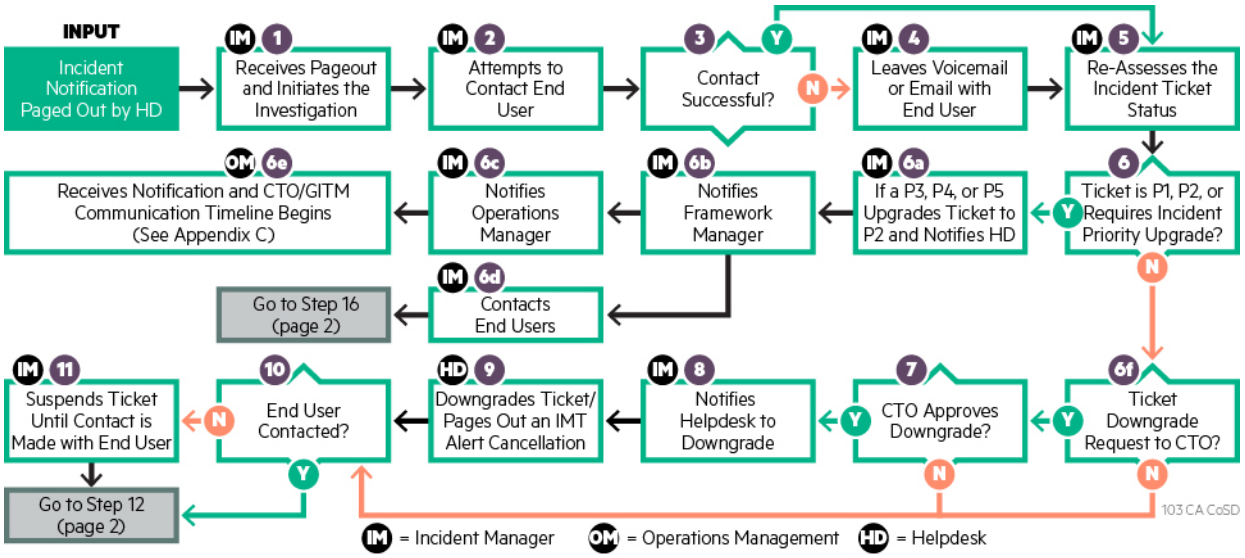
HPES will continue to provide full life cycle IM using our existing processes as stated above and described in detail below. One major change going forward will be the addition of SDMs as key positions in the Contract. Each SDM will be assigned to a County business group and led by the enterprise SDM. 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

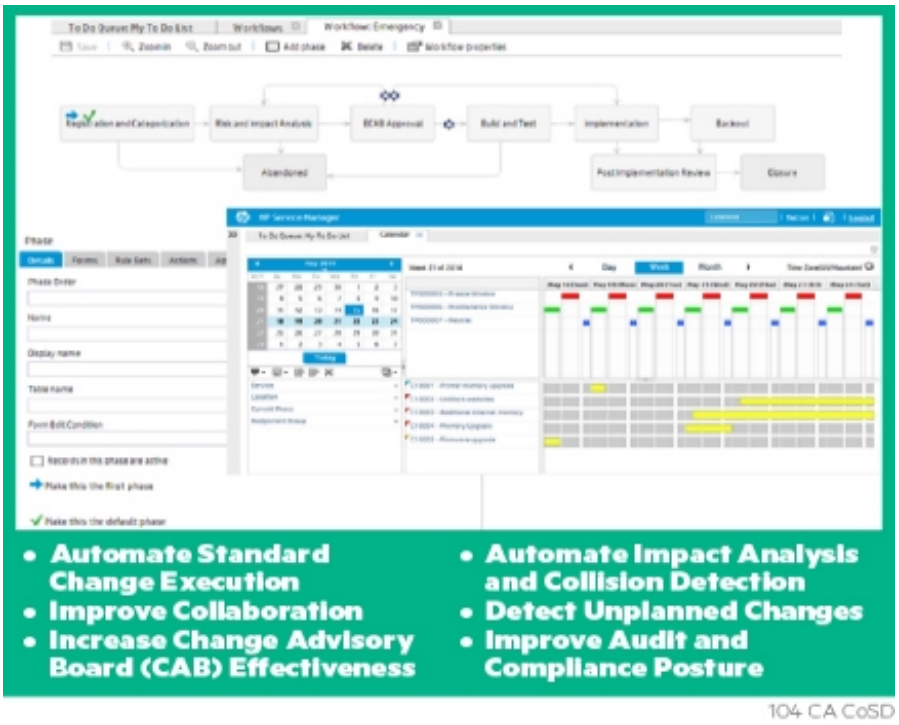
Operating out of our Rancho Bernardo facility, the HPES Change Manager will implement and sustain repeatable, methodically driven change management processes and best practices. Timely, accurate, available stakeholder documentation is an integral part of the change manager's activities, which we will 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.

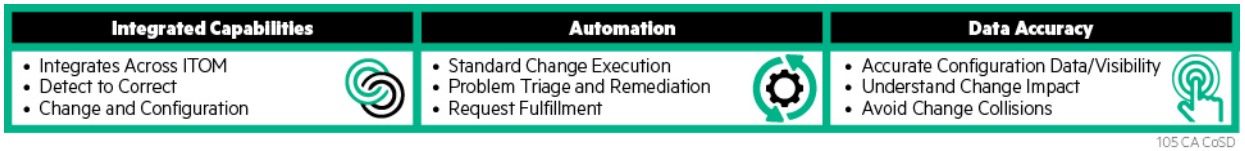
A notable Suite feature is its global forward schedule of change that brings change requests together into a unified common view, providing improved visibility and planning. Change calendars are based on multiple views—including an Outlook-style calendar with timelines by month/week/day/hour, by application, 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.

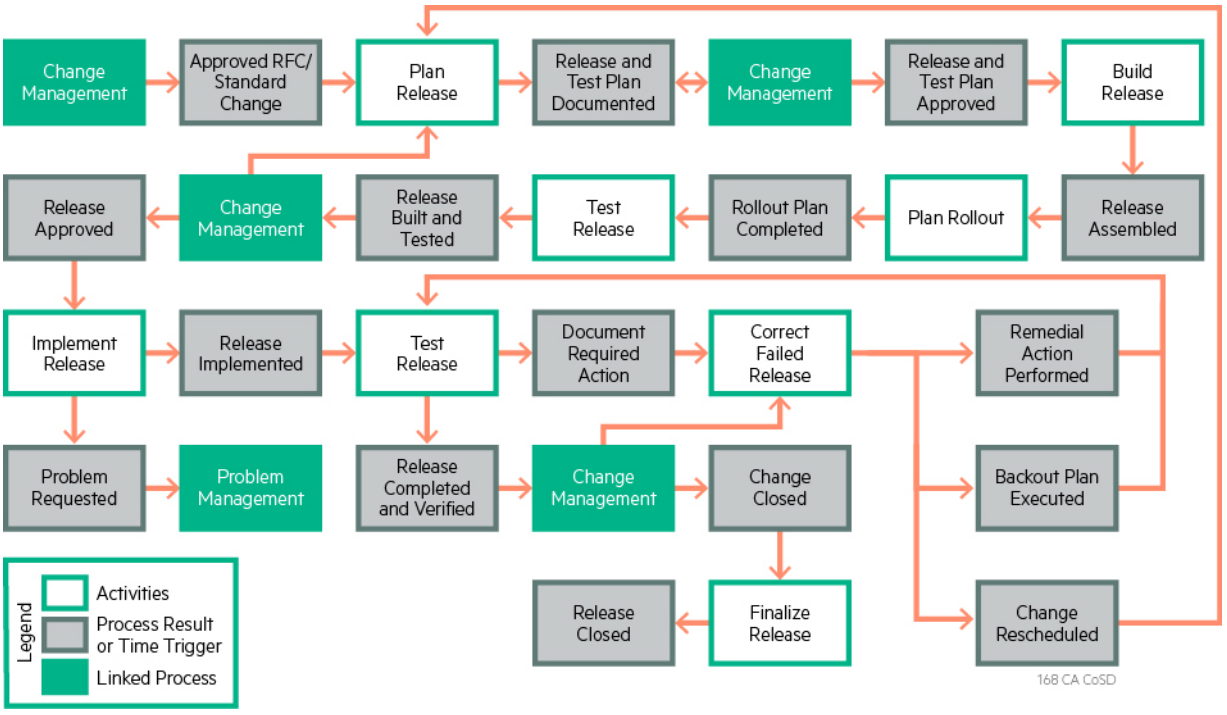
Release management is the process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. Its primary objective is to protect the integrity of the live environment and to make sure that the correct components are released.

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.

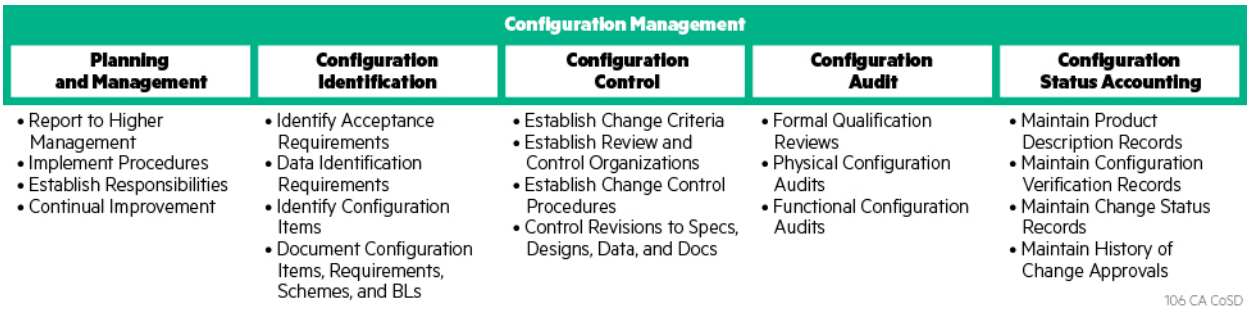
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

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.

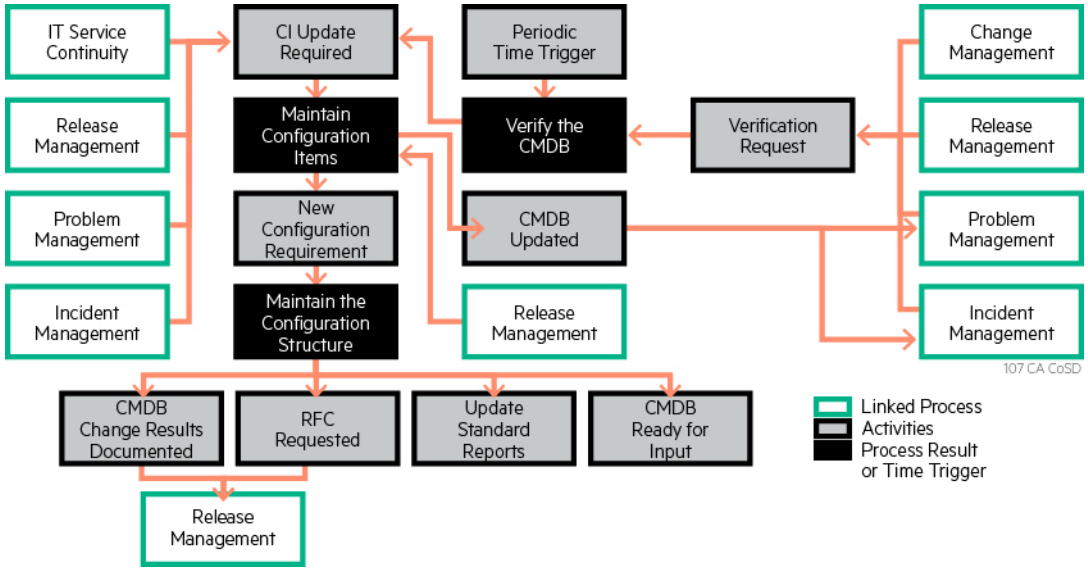
The primary purpose of CM at the County is to make certain that product attributes and technical baselines of all software and systems in use by the County—collectively known as configuration items (CIs)—conform to the documented design for each released software version. This includes the means to document, 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.

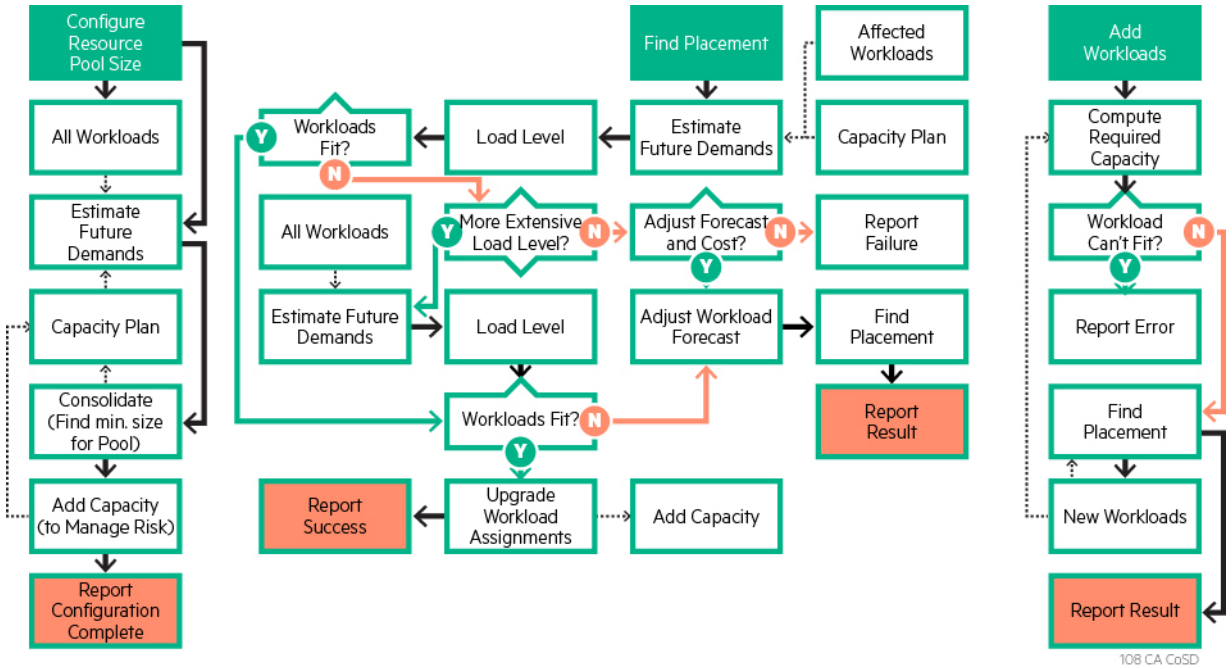
County employees with access to the Service Portal may view the capacity reports at will, giving them the freedom to access data and reports as required. They can export reports to Adobe Acrobat, MS Excel, MS Word, or Rich Text format, enabling further analysis, combining with other data, or including 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

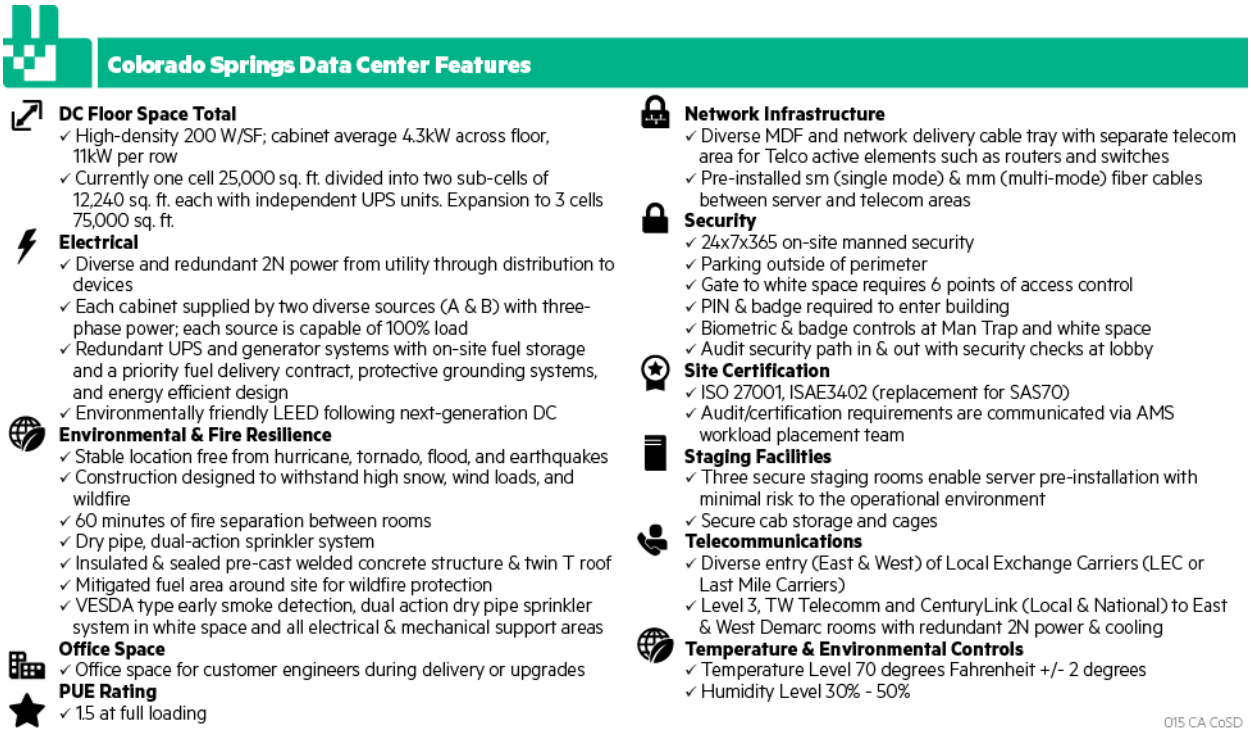
We have selected our Colorado Springs, CO Data Center (CSDC) for the County's recovery site, connected via dedicated 10GB circuit, providing data replication. We will be able to provide a wide variety of disaster recovery services—dedicated to shared and/or hybrid solutions—at this central location.

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

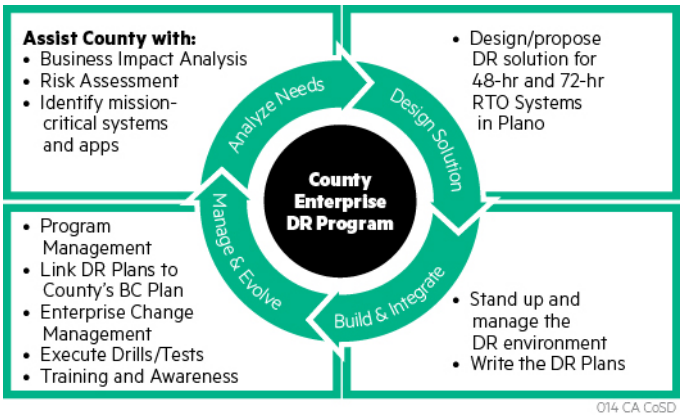
HPES takes a holistic, yet modular, approach to manage the County's enterprise DR program, as depicted in Figure 27 The methodology is comprehensive, derived from decades of experience, and is built on industry best practices and standards of the Disaster Recovery Institute International (DRII) and ITIL. 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

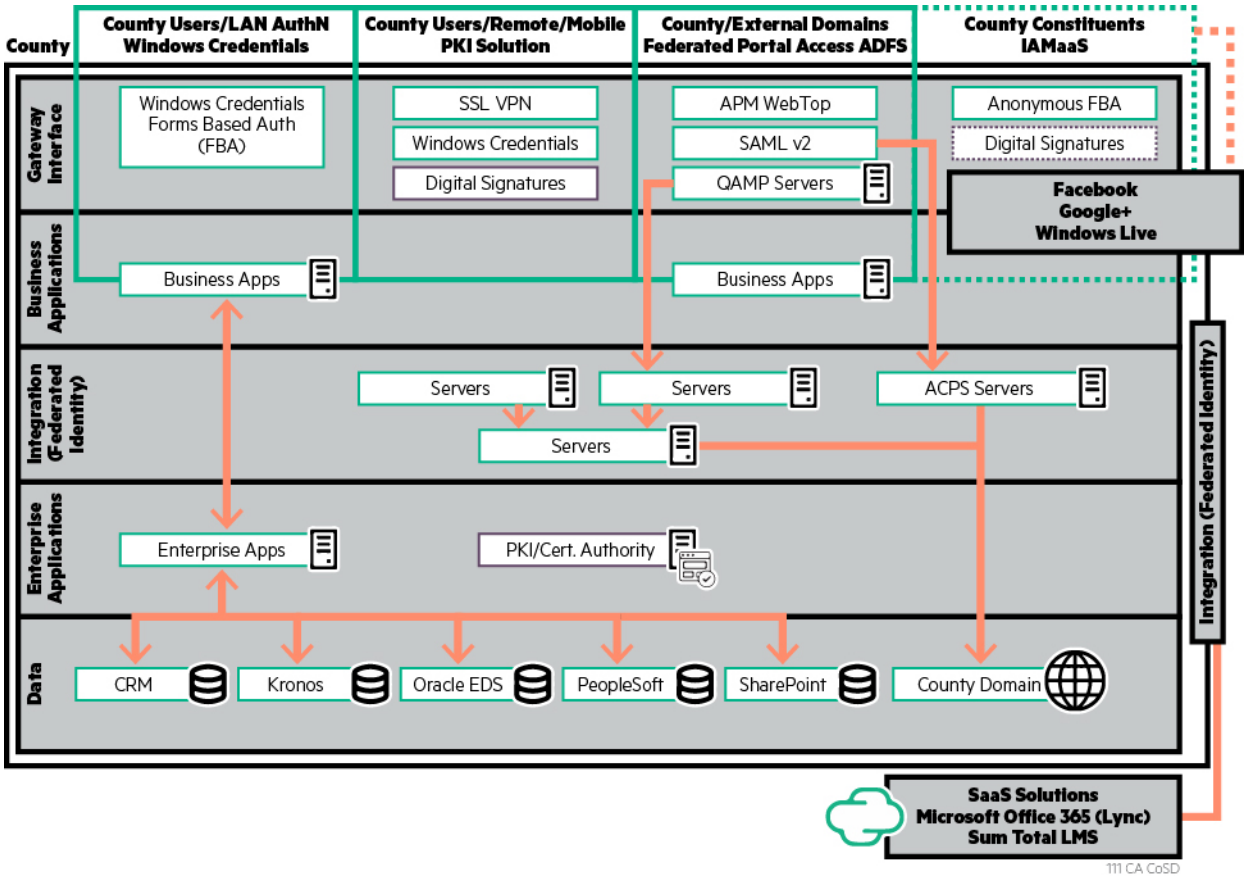
approach makes certain that access privileges are granted according to a singular interpretation of policy and that all individuals and services are properly authenticated, authorized, and audited. Recognizing the critical importance of IDAM, particularly in light of emerging technologies and cloud-based 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.

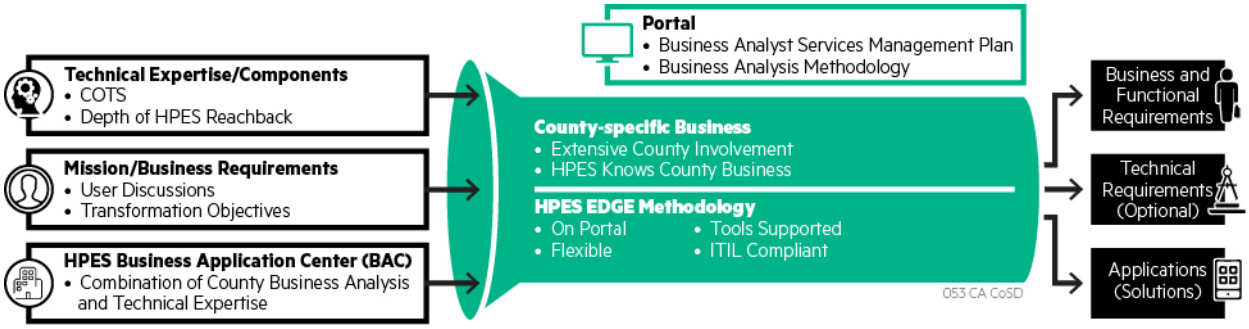
- Methodology & Key Processes – Key methodologies and processes in proposed solution including year-to-year continuous improvement

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.

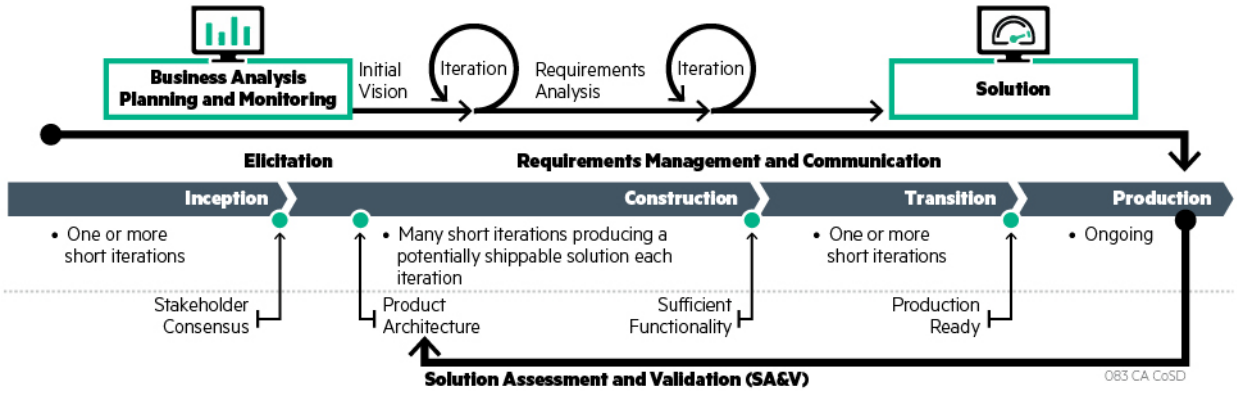
This approach starts with the Business Functional Requirements Document. Our proposed approach is:

- 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.

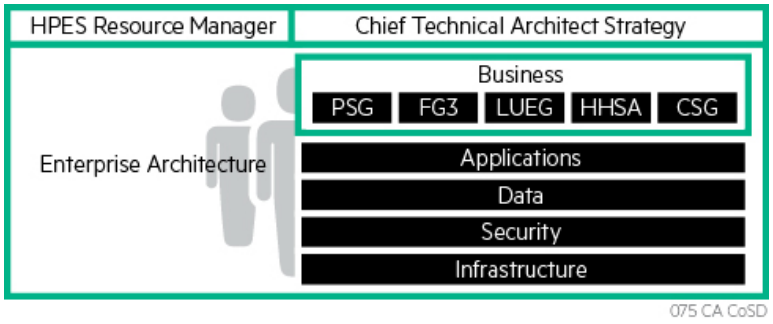
The CTA provides the bridge between the deeply technical domain architects, business analysts and solution architects and other subject matter experts to ensure that the technology infrastructure meets enterprise goals, such as adaptability and complexity reduction. CTA shall work closely with Business 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

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 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.

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.

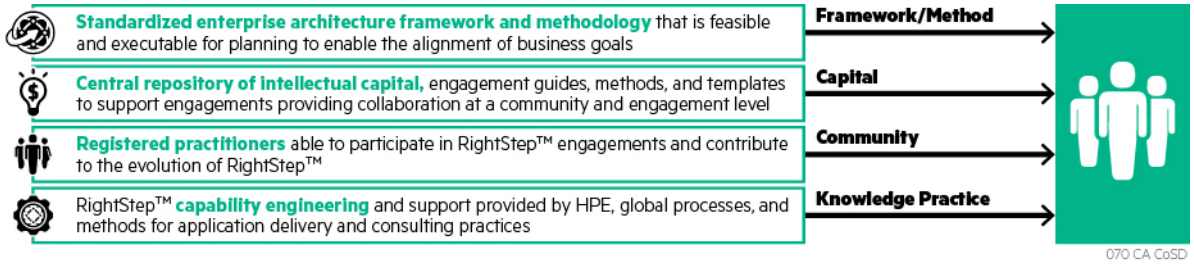
SECTION TITLE	CONTENTS
	<Template Sections 4.6.1 can be combined or split in two to describe the current and proposed security architecture>.
Acceptance Criteria	<Describe the success criteria and acceptance requirements guidance. This is at high level, acceptance test plans are created later in the 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.

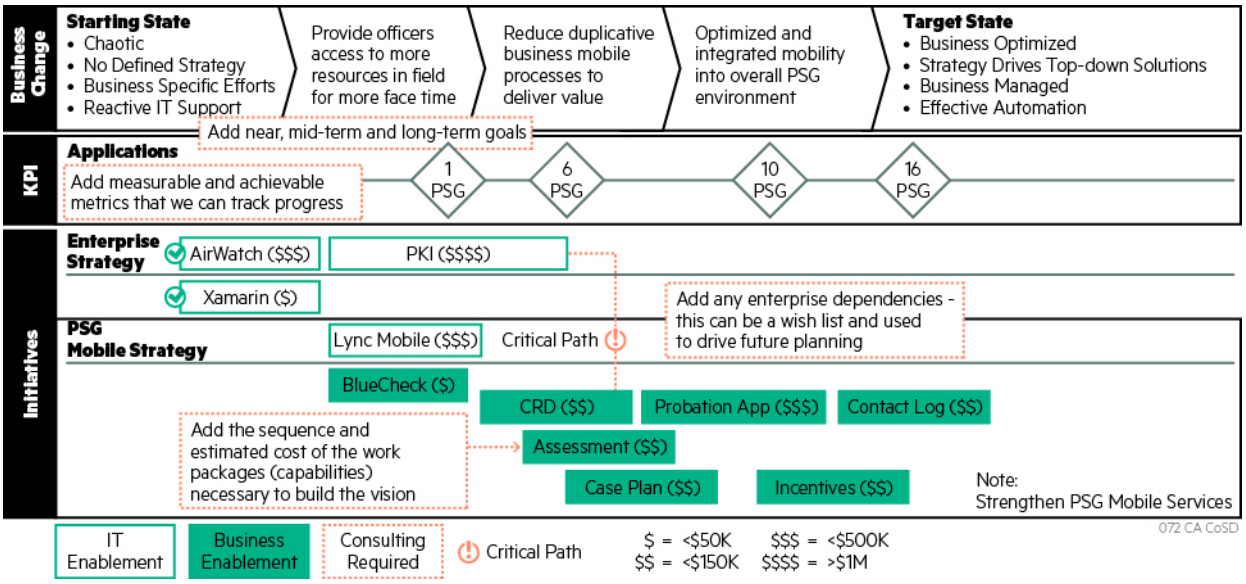
Tools, methodologies, and accelerators are used together, as detailed in Section 2.5.6.1, from HPES' Enabling Delivery and Global Excellence (EDGE) Platform Architecture Suite standards.

- 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

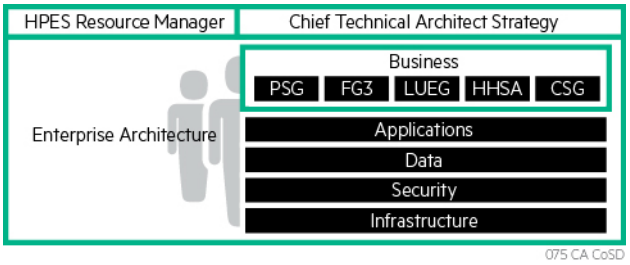
The on-call rotation in which the SDMs participate is critical to facilitate centralized after-hours support to the County for issue resolution as well as making sure each SDM has appropriate amounts of time off and vacation as required. HPES is proposing five SDMs who will rotate on-call every five 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

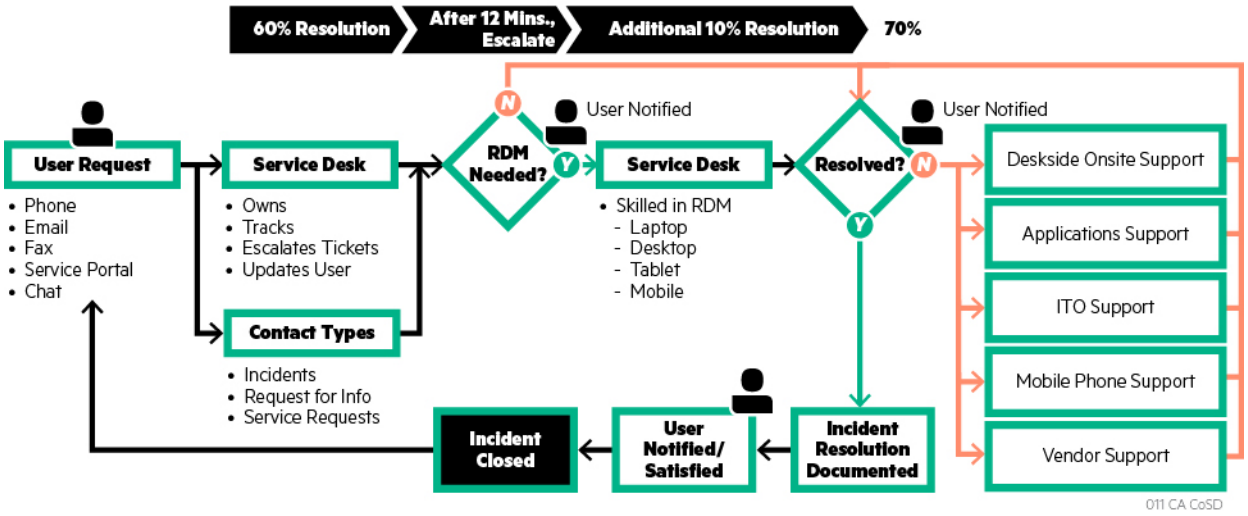
Service Desk. The HPES approach to Service Desk is rooted in the ITIL framework, focusing on repeatable, scalable processes and continual process improvement. In Figure 37, we show the Service Desk full life-cycle ticket ownership and end-to-end tracking of all incidents and SRs for all County End Users 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

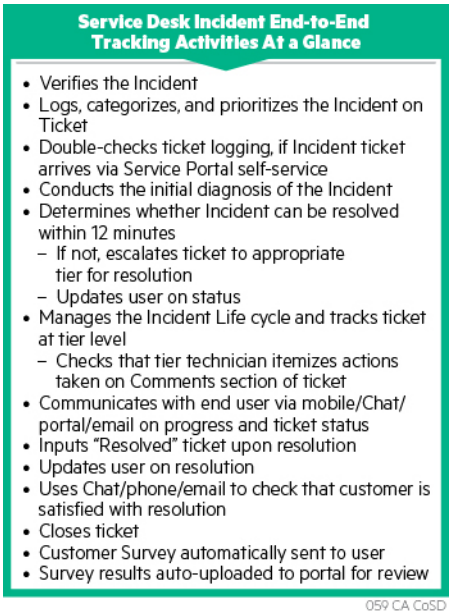
Service Desk has ownership of all tickets and tracks them from user submission through ticket resolution. We have implemented ITIL-aligned processes enabling any Service Desk agent to check on ticket status even if it has been escalated to other resolver groups for action. The Service Desk agent can 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.

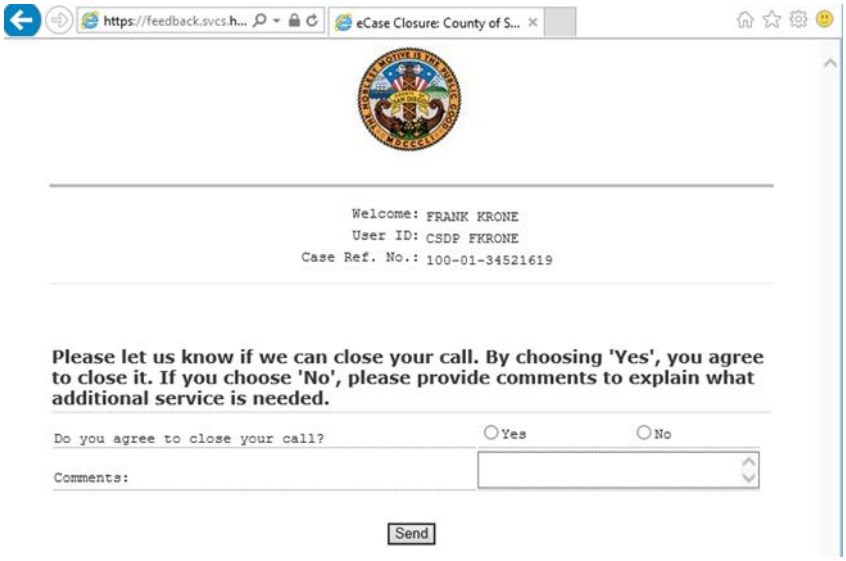
Subject Matter Expert (SME) Escalation. When the Service Desk agent recognizes that the source of the Incident requires SME support, he/she escalates the ticket to the SME support team appropriate to the affected framework (e.g., Applications M&O team, Network team).

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.

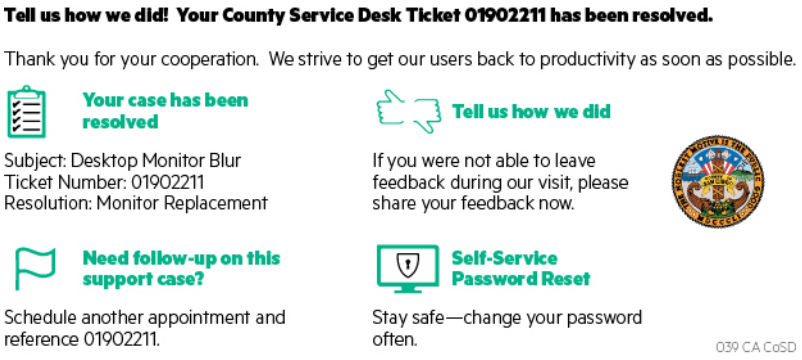
Ticket Closure. Once the ticket is resolved, the resource responsible for the resolution changes the status of the ticket to "Resolved." This action automatically notifies the user via email of the resolution, as shown in Figure 39. The body of the email requests a reply within 3 days if the issue was 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.

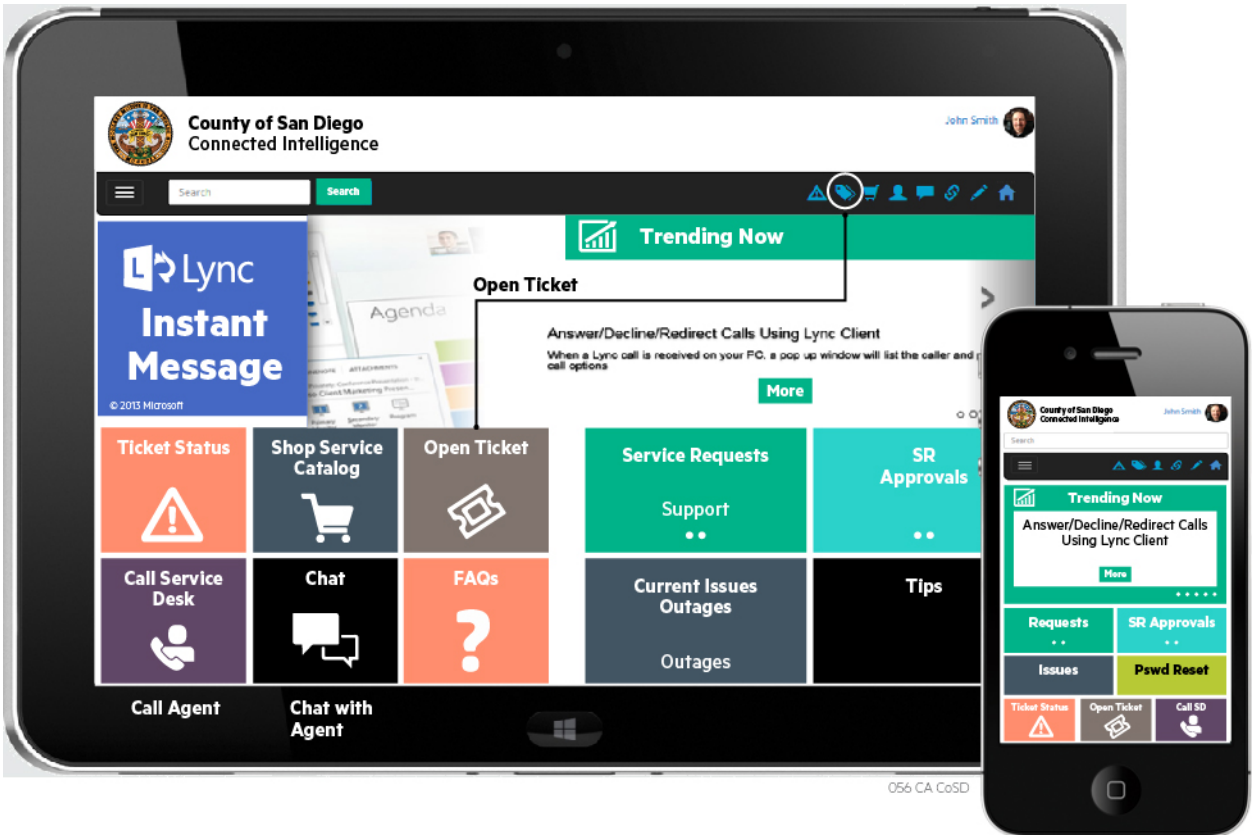
Self Service for Incidents/Problems. Similarly, the new self-service ticket capability option enables an End-User to open a non-critical ticket that is automatically submitted to the Service Desk queue for review and action. The user clicks on "Open Ticket" to submit hardware, software, connectivity, 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.

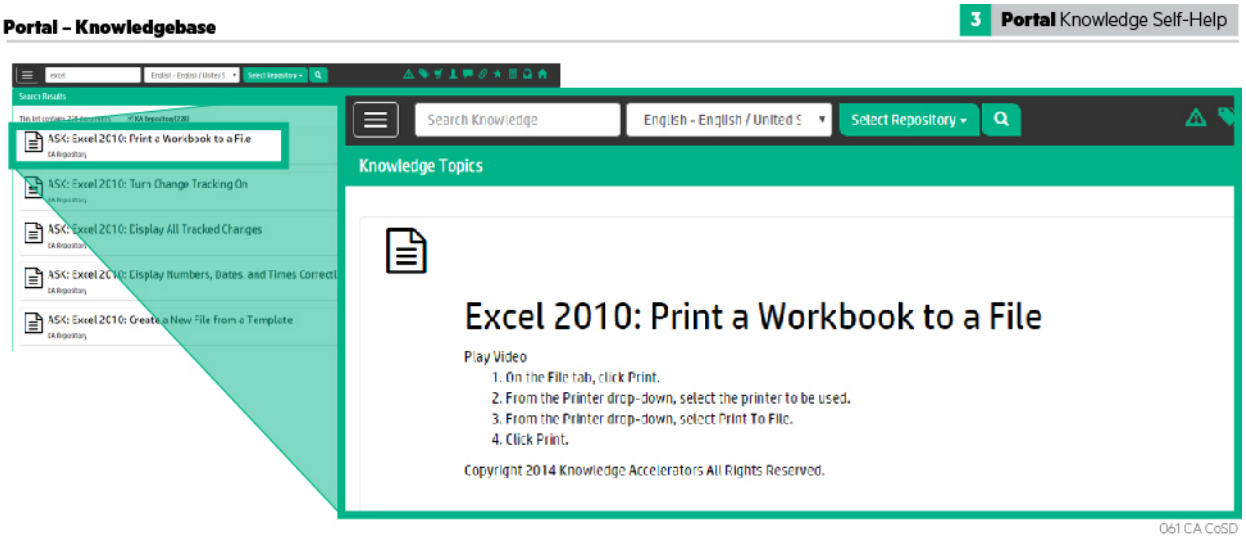
We look forward to working with County stakeholders in developing the branding, look, and feel of the portal as well as expectations of functionality.

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.

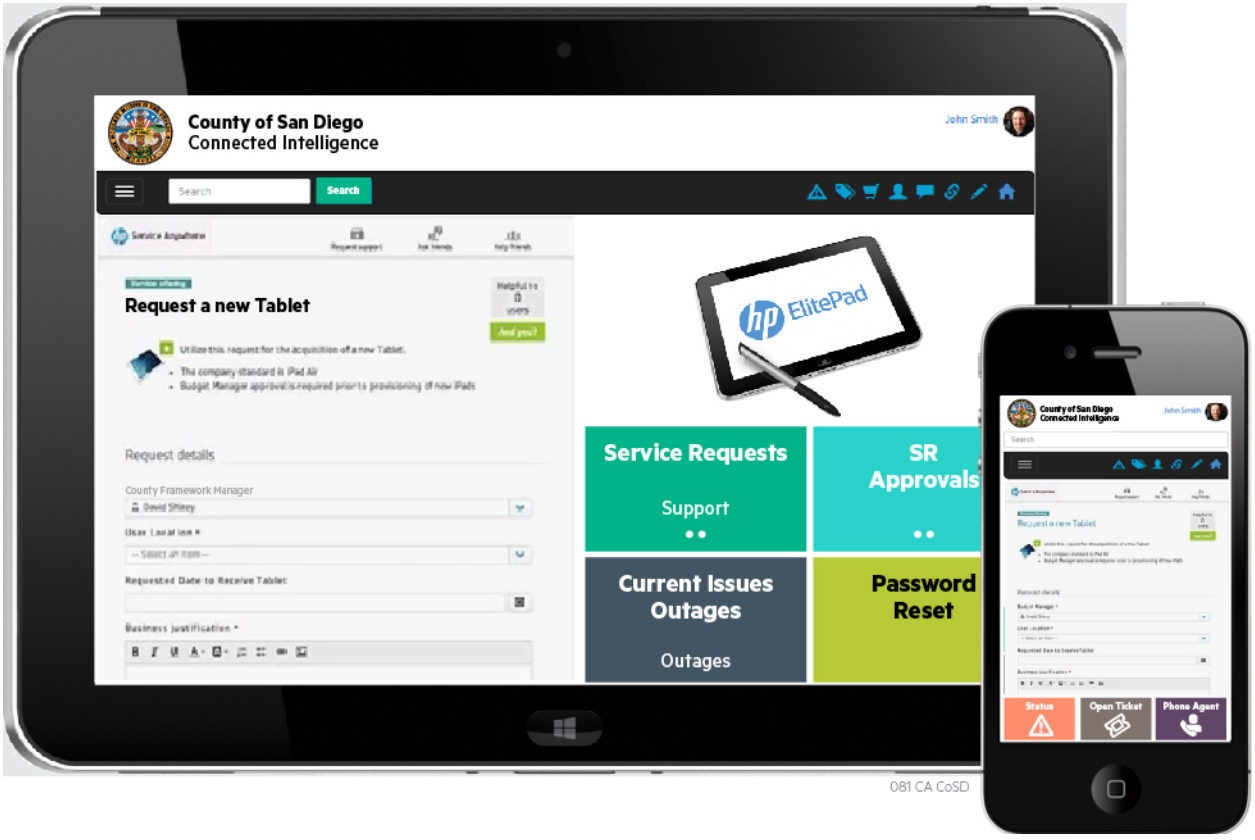
Service Requests by Self-Service. Once the Service Portal is implemented, the user will be able to make SRs on user-friendly SR forms that are routed to the Service Desk ticket screen (in accordance with the approvals granted by the County). A Service Desk agent will be assigned the SR that arrives from 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)

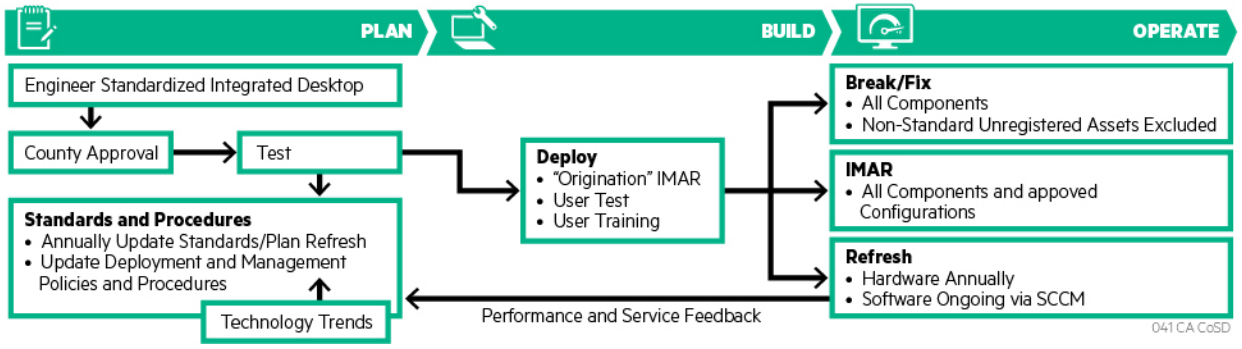
- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches

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



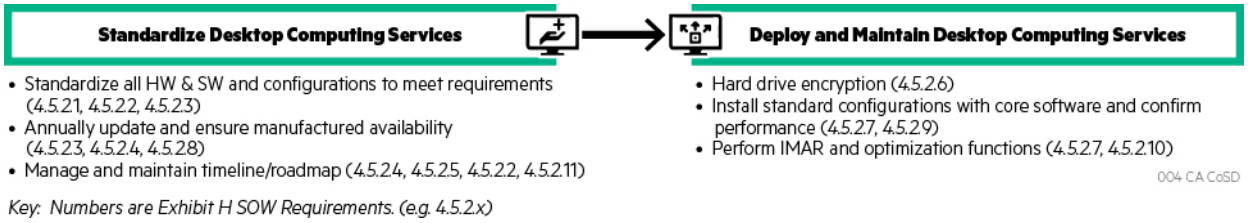
We manage the desktop services and architecture as an integrated solution across the Plan, Build, and Operate life cycle structure.

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.

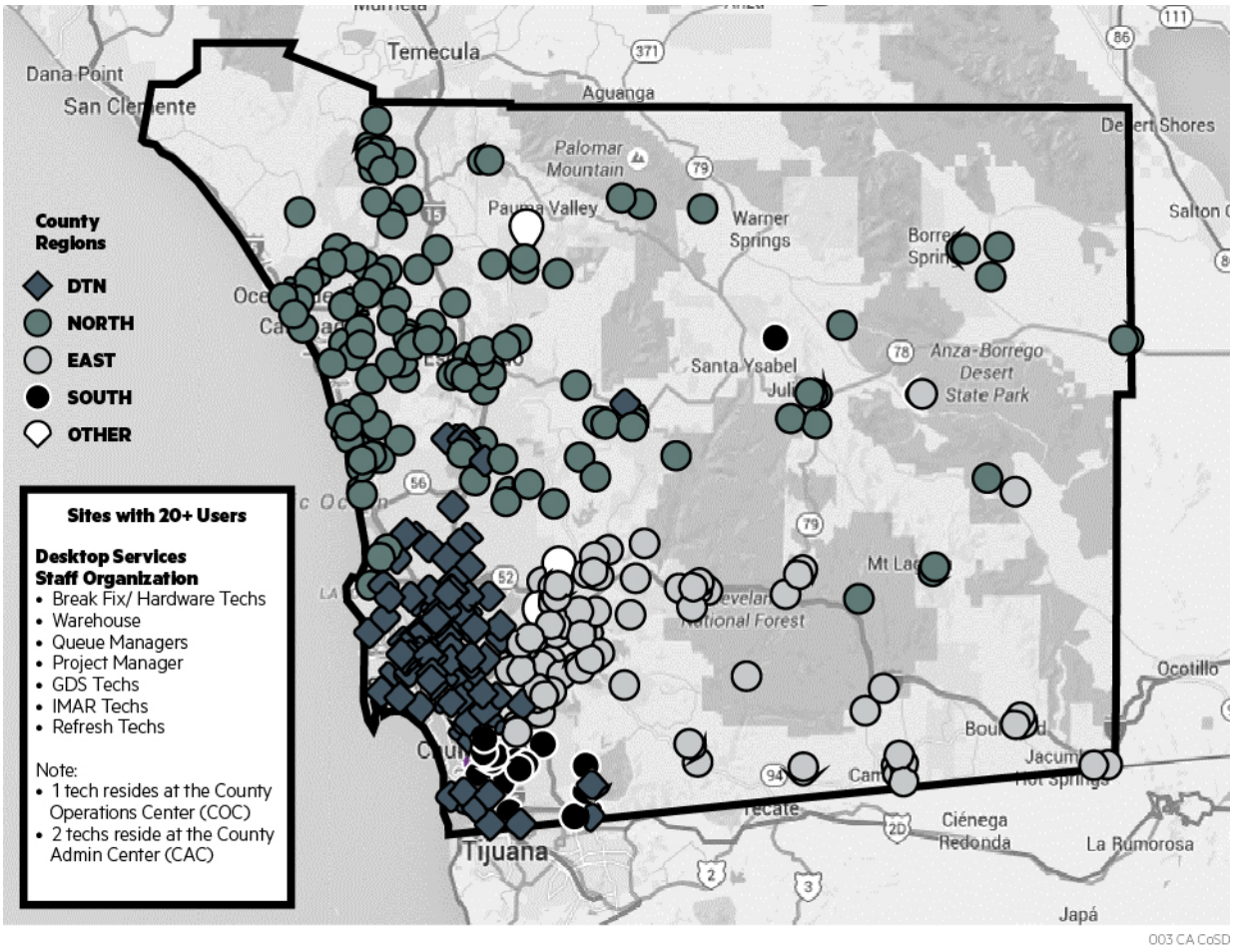
We staff the core hours of Monday through Friday 6:00 a.m. to 6:00 p.m. with a full shift. Non-core hours are staffed at levels sufficient to provide necessary service as required over the weekends, on holidays, and after the business day. Our support service levels are available 24x7x365. Online ticket 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.

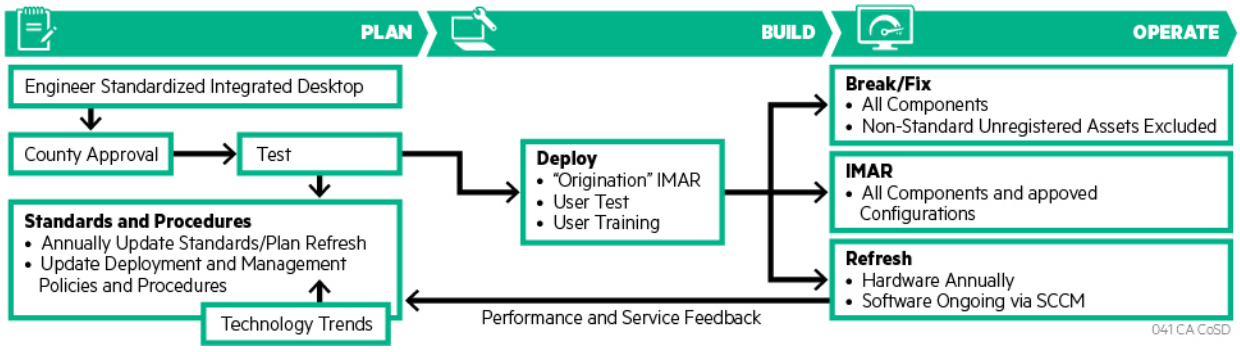
In addition, we provide communications to our service technicians to keep them up to date on the County's mission via all-hands meetings, webinars, leadership briefings, weekly/monthly newsletters, knowledge shares, and other County specific activities.

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.

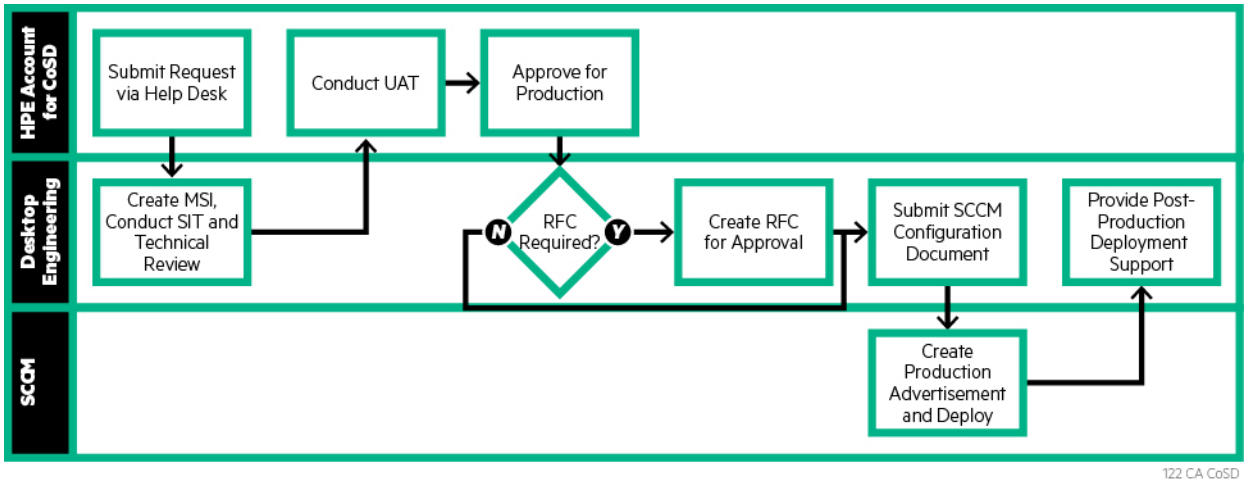
- The technician performs the foundational set of system and end-user testing, which is a series of standard tests.
- Technician logs the fix, updates the asset inventory (if necessary).
- Upon completion of the service, the technician moves on to work their next ticket

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.

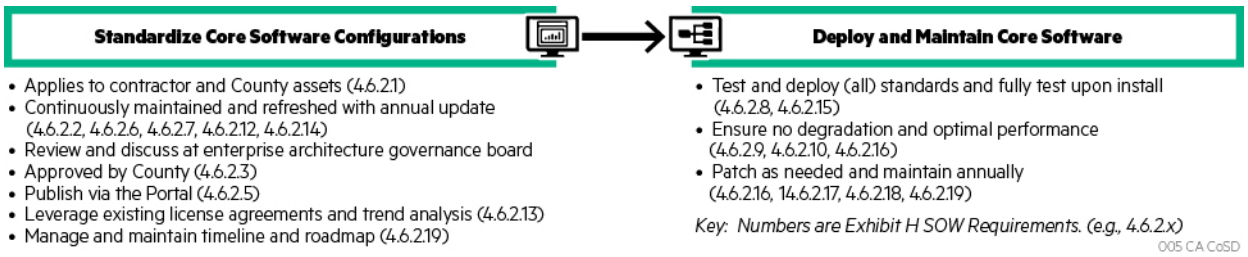
None.

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

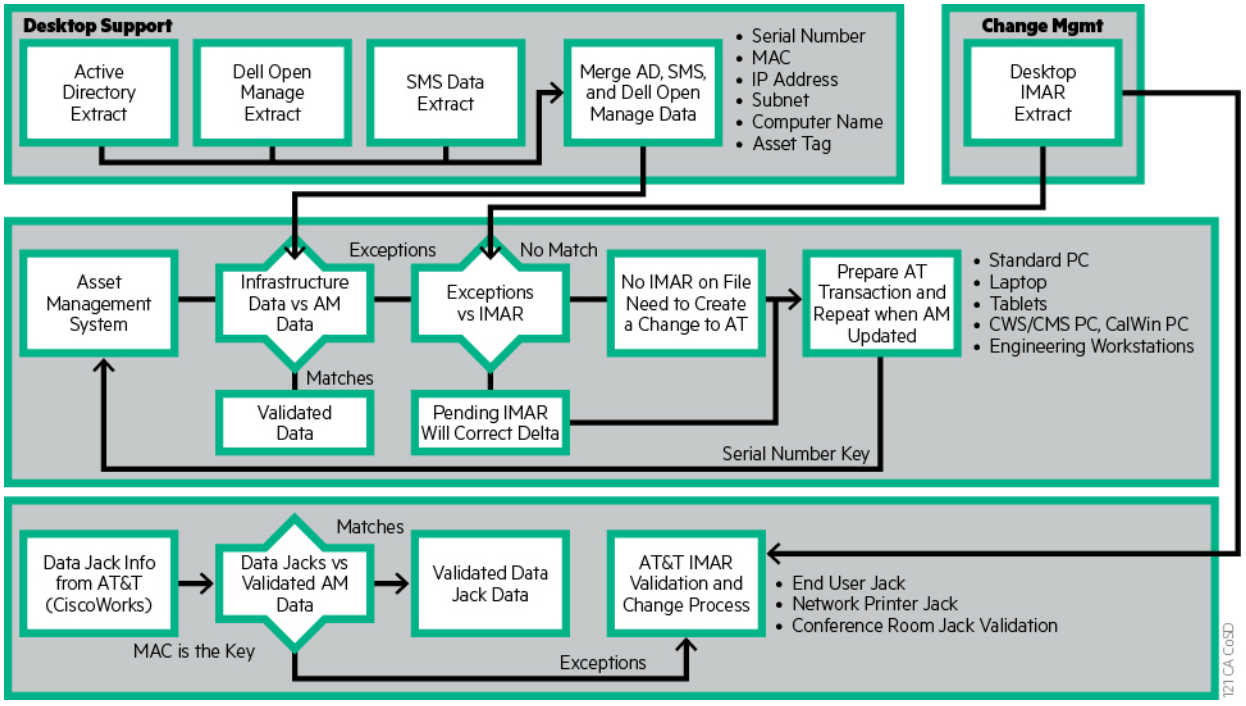
architecture meeting, the annual standards review, catalog review board, and other forums, we are confident we will continue to bring optimal value to the County.

- 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.

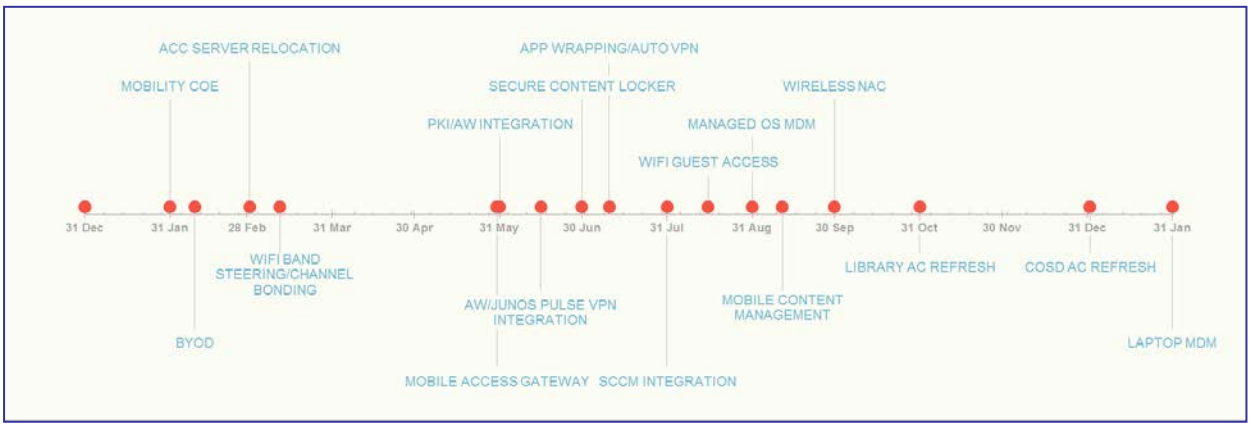
None.

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

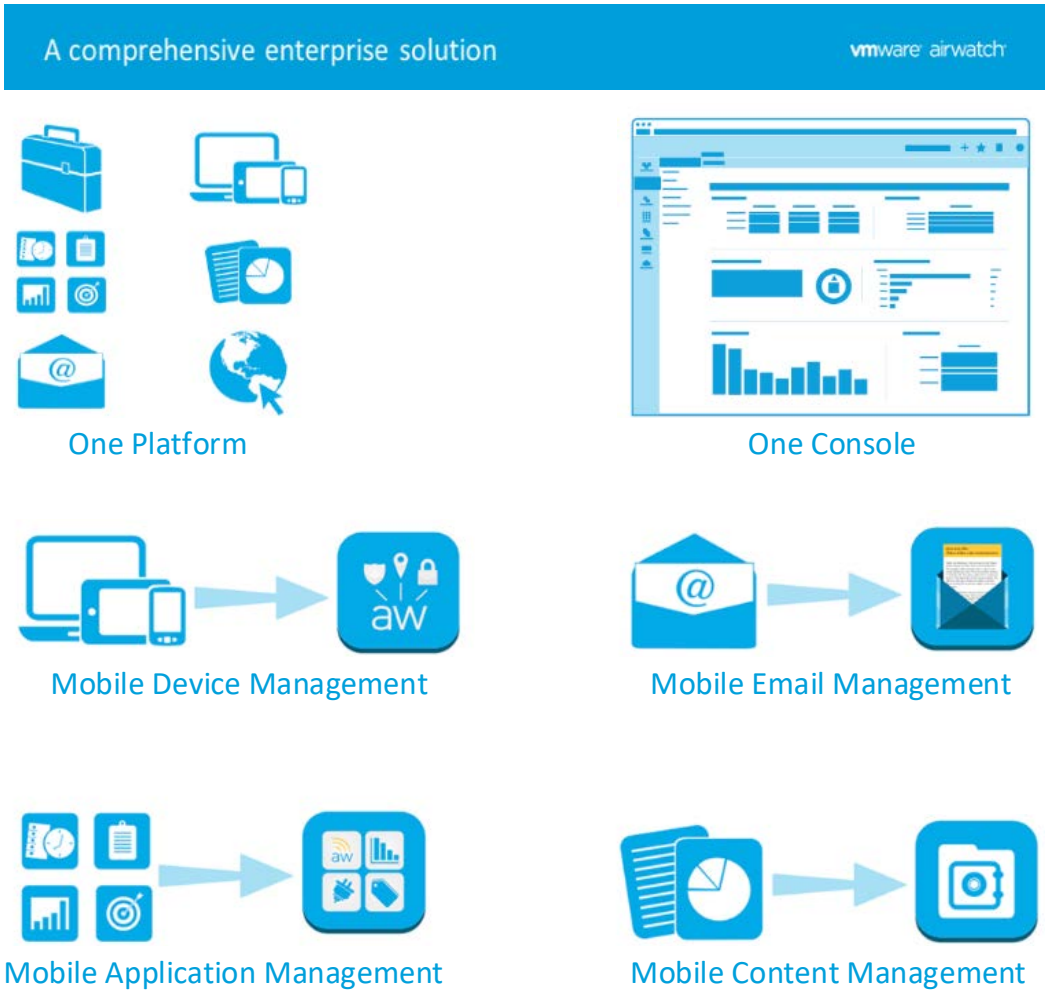
More than 3,800 County users are using the AirWatch Mobile Device Management (MDM) offering and associated support services. MDM provides policy enforcement and email access to smartphones and tablets, plus distribution of public and custom mobile applications through the County mobile application store 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

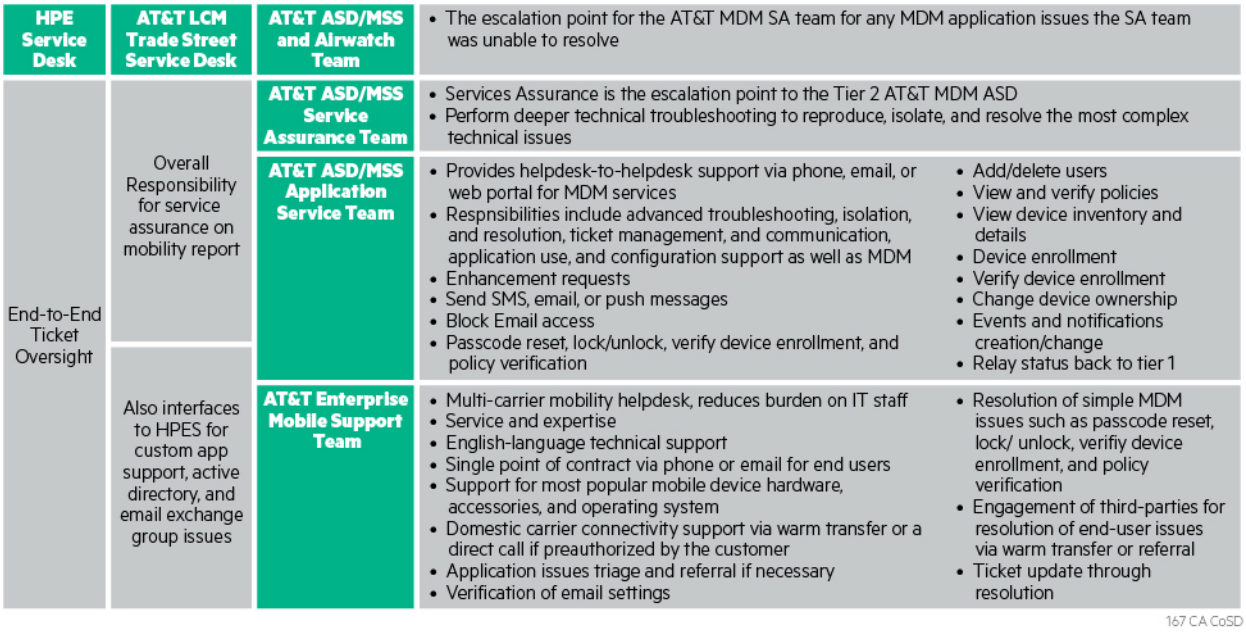
This is the first-level technical escalation point to the AT&T MSS Application Helpdesk, which performs deeper troubleshooting to reproduce, isolate, and resolve the most complex technical issues.

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

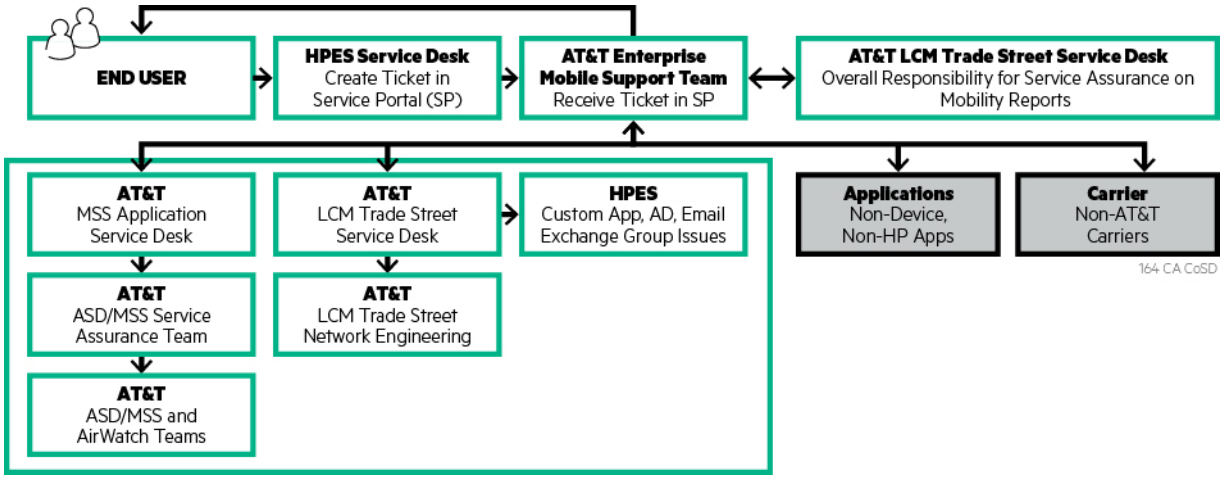
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

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.

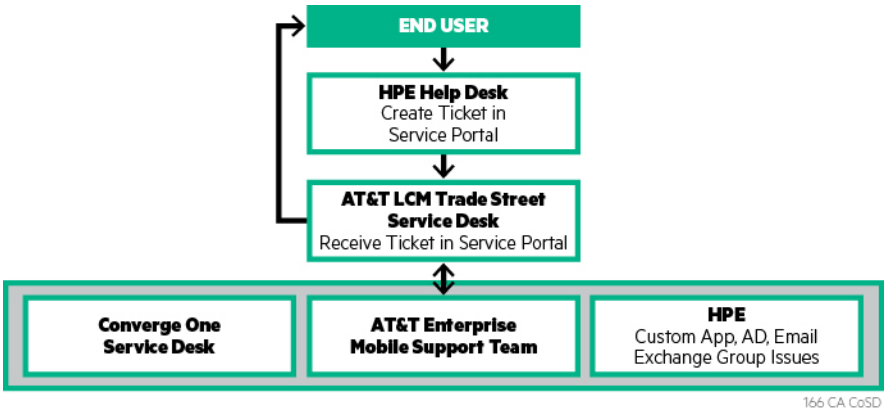
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

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.

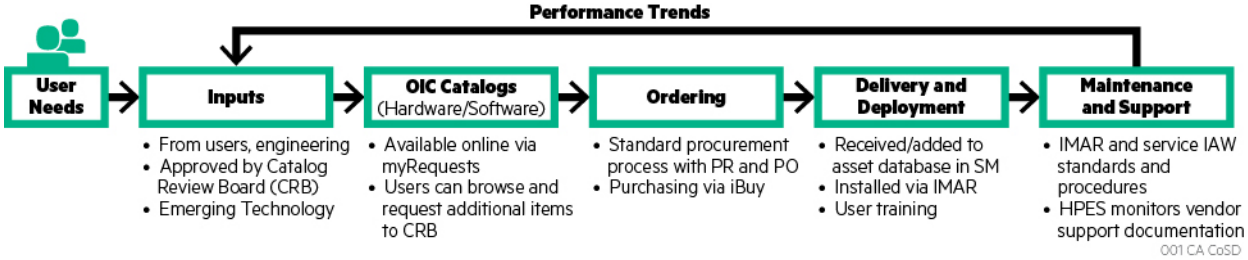
To implement this solution, the configuration of the catalog will be controlled by the Catalog Review Board (CRB). The board consists of HPES and County selected points of contact (POCs) from each department to discuss, review, and approve items for inclusion in or removal from the catalog.

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

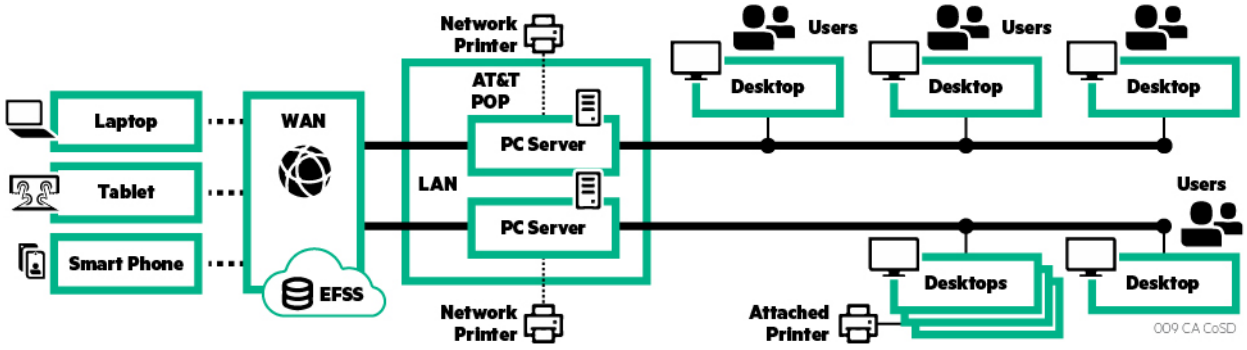
PRINTER TYPE	QUANTITY SUPPORTED (AS OF MARCH 2016)
Monochrome Network Workgroup Printer – Standard Format	735
Monochrome Network Workgroup Printer – Large Format	52
Monochrome Network High Volume Printer – Large Format	19
Color Network Workgroup Printer – Large Format	45
Color Network Workgroup Printer – 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).

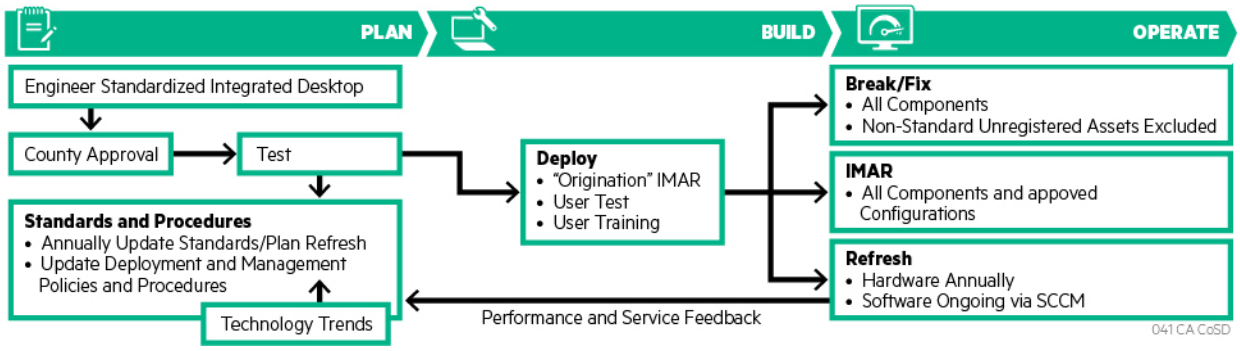
Because this question relates to "mitigating impacts to existing systems while transitioning to new standard platforms" our response focuses on our annual update and refresh activities. In our answers to the first three questions (2.7.1, 2.7.2, and 2.7.3) there is significant overlap in our approach 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.

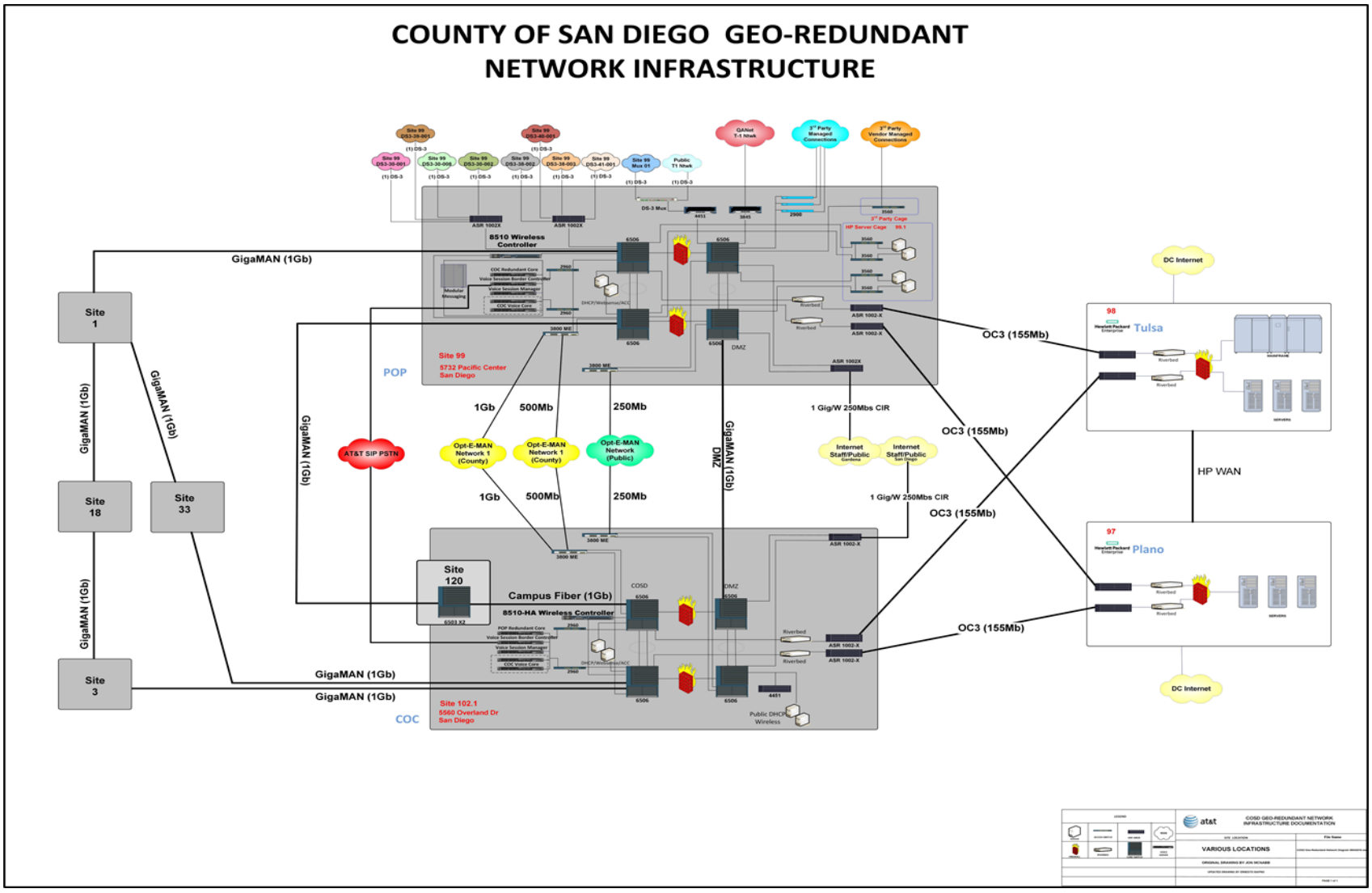
Upon activation of our approved solutions, we employ several automated tools to maintain an accurate and up-to-date inventory of all hardware and software supporting data network services. In addition, we use automated tools to continuously monitor the provisioned services from an operational and bandwidth 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.

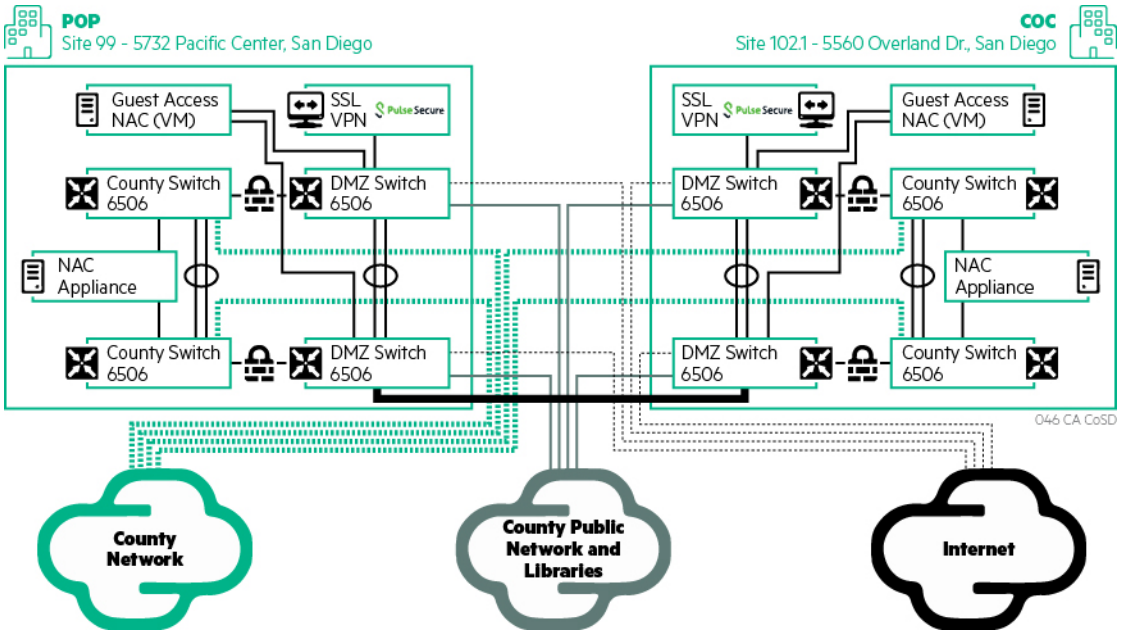
Continuous Improvement

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

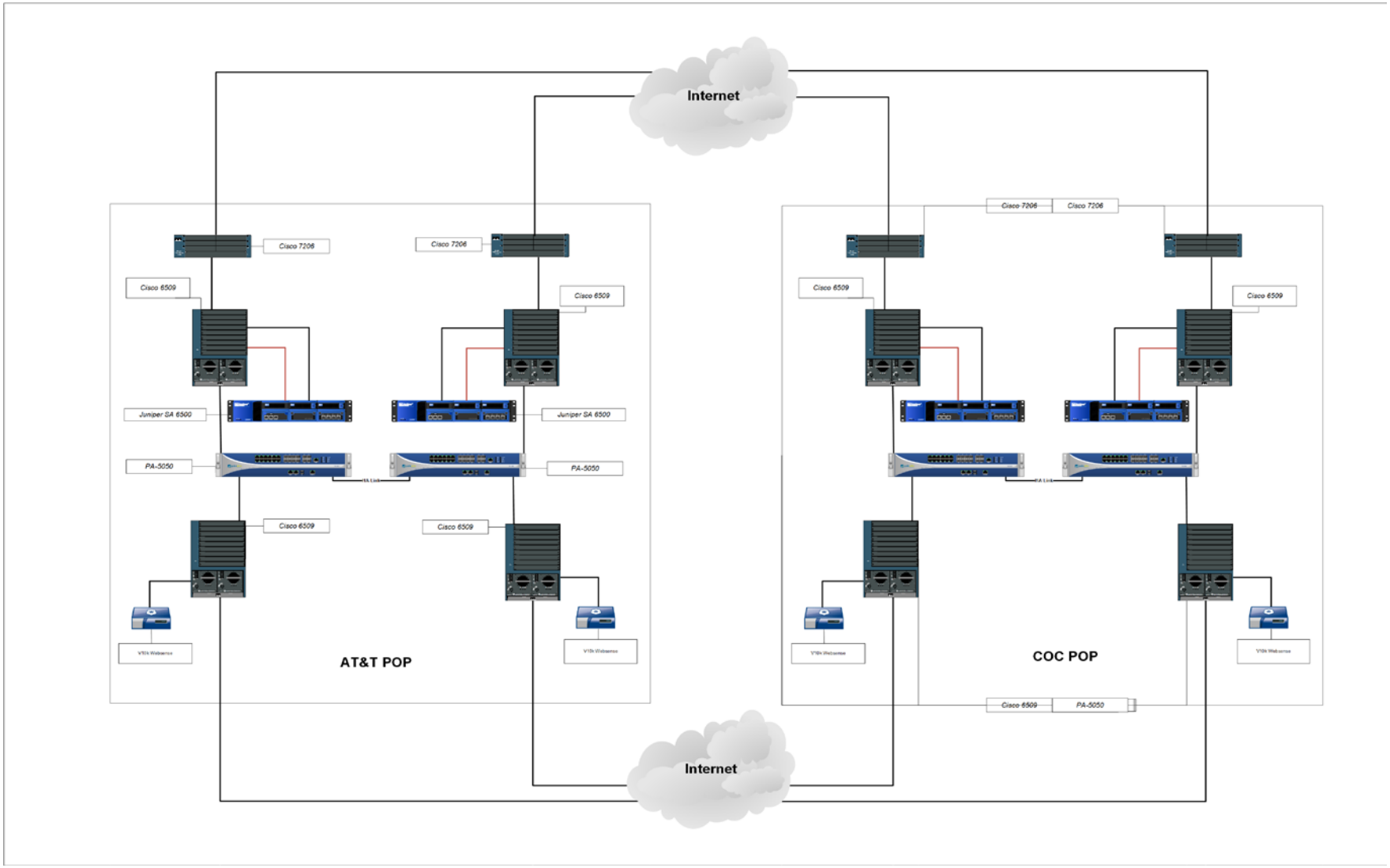
Using the PulseSecure client loaded on the County-managed laptops (as well as managed mobile devices once that project, which is currently in flight, is completed) allows full network access to any and all resources available to the user when connected on the County LAN. This client-based connection 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.

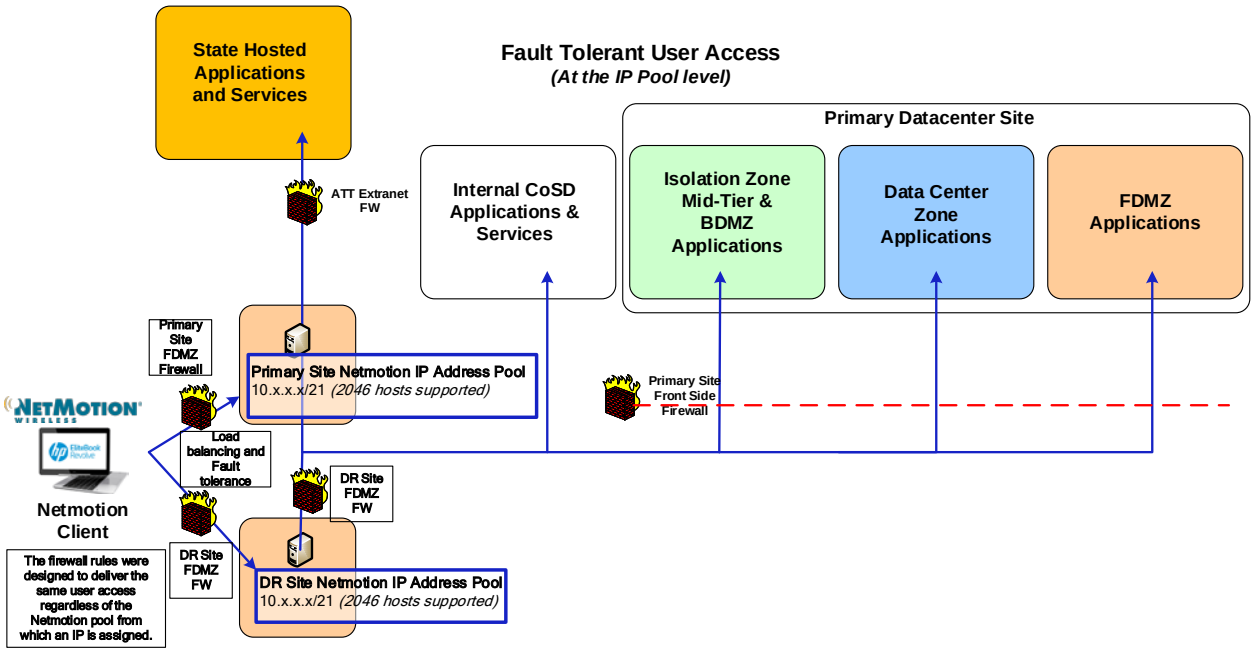
Currently the Pulse Secure mobile client is not "connection aware" and is unable to dynamically reconnect to a secondary gateway in the event the connection to the primary gateway fails. The Contractor has initiated feature requests and roadmap discussions with Pulse Secure to address the manual failover 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.

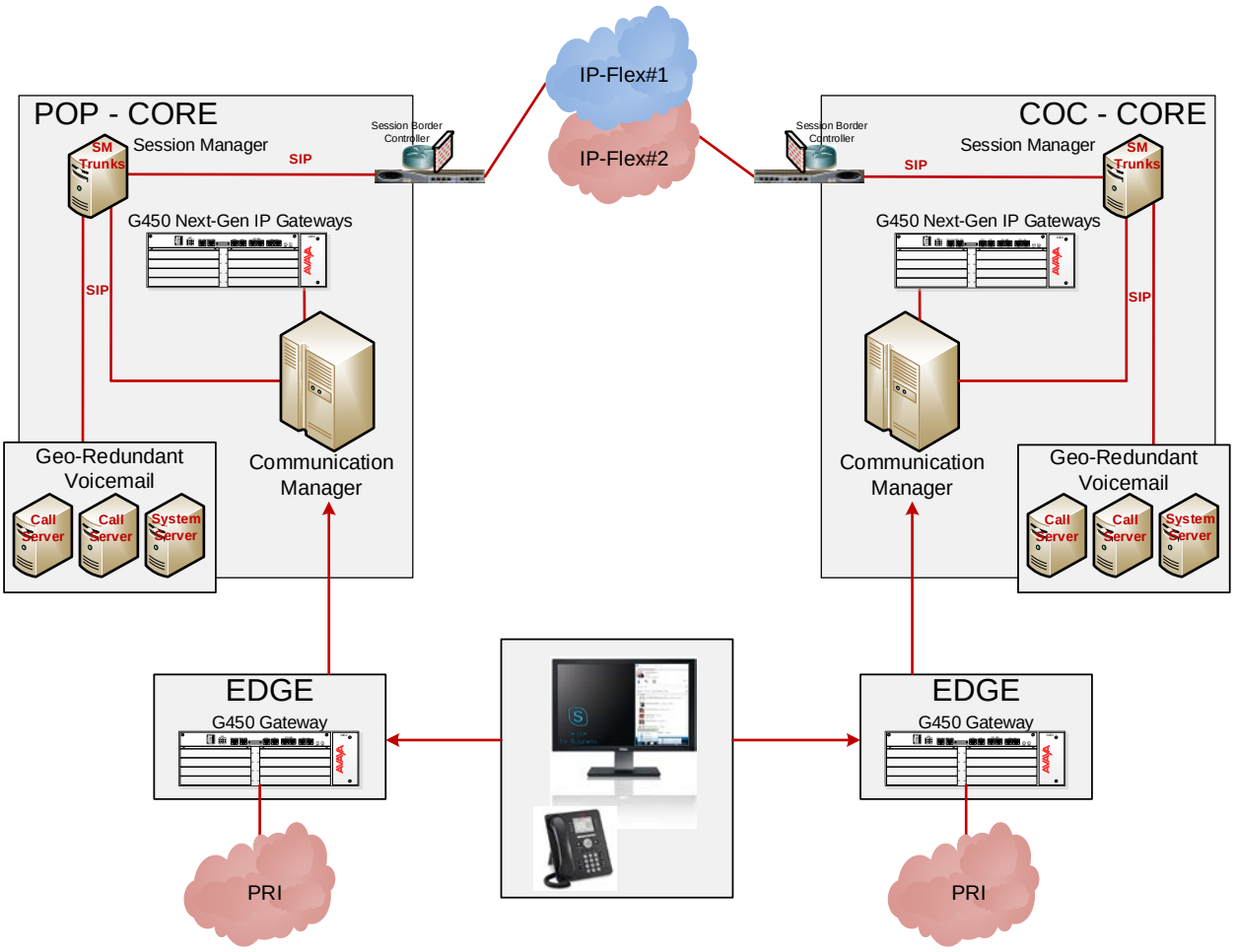
As a part of this upgrade to VoIP each site will also be migrated to a new E911 service, so that first responders have the necessary site and call location detail in the event of an emergency.

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.

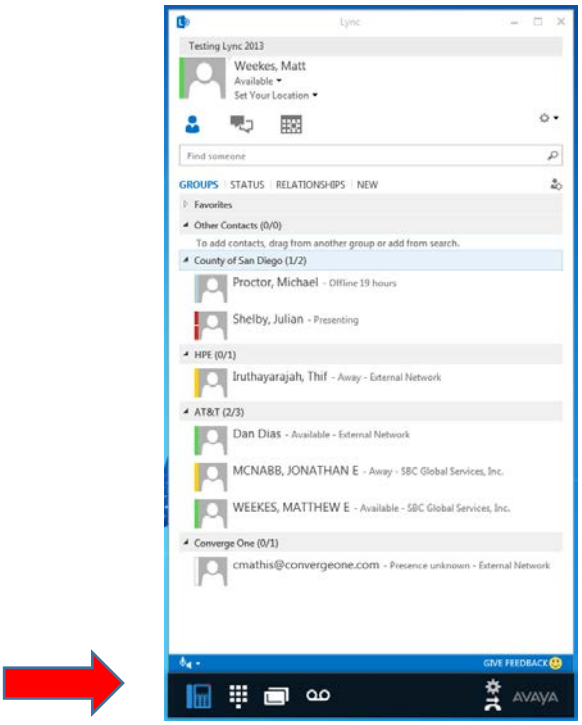
Unified Communications

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.

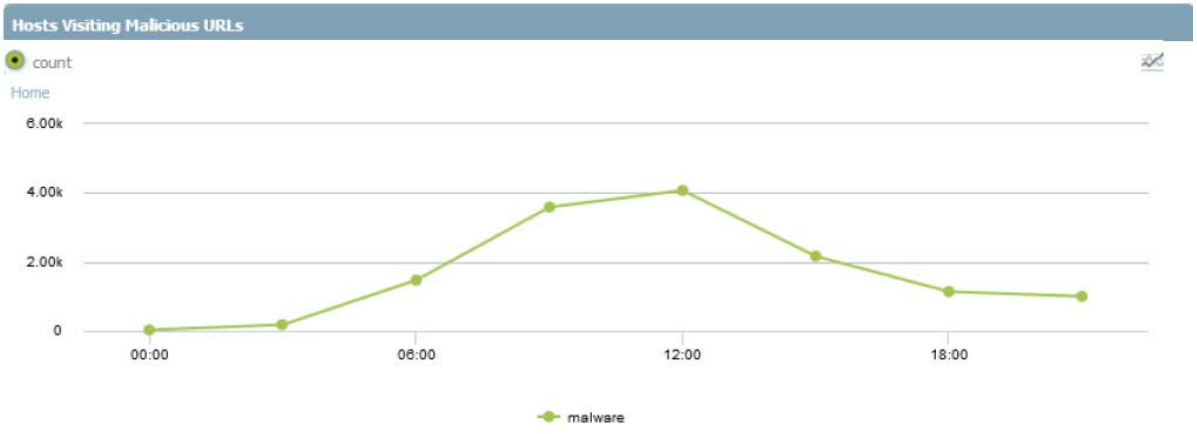
Figure 68. Security Reporting



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.

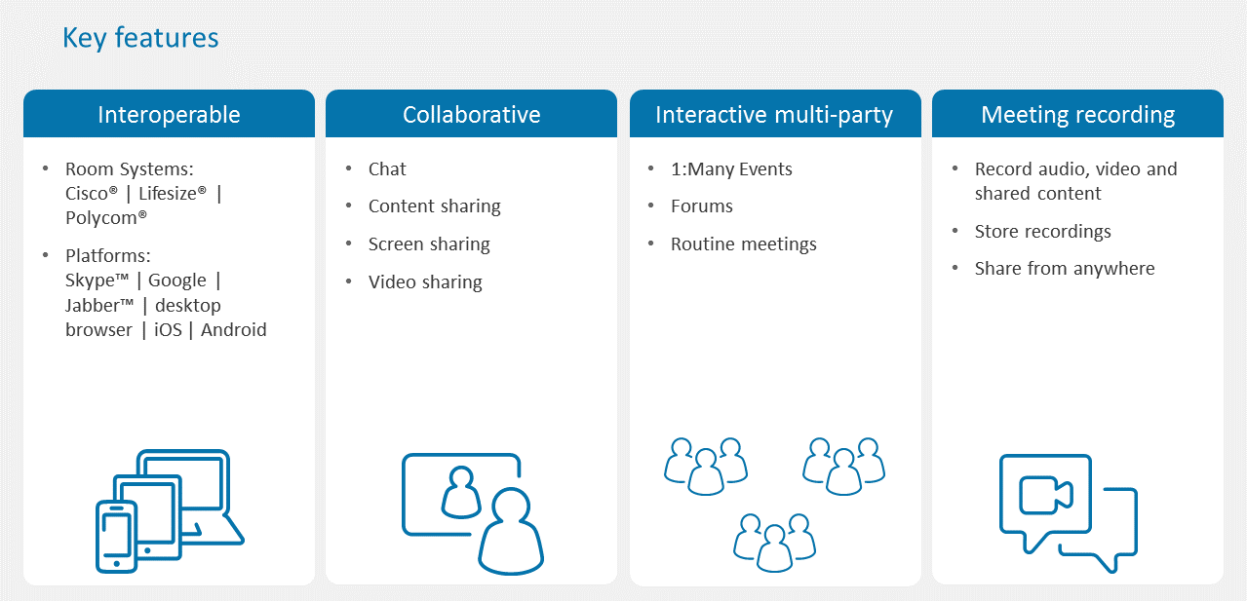
With the expansion of desktop and mobile client-based video functionality, there is increased business value in enabling cross-platform video conferencing systems. With such a system, video can become a more pervasive means of meeting with County employees and constituents. To meet these emerging needs 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.

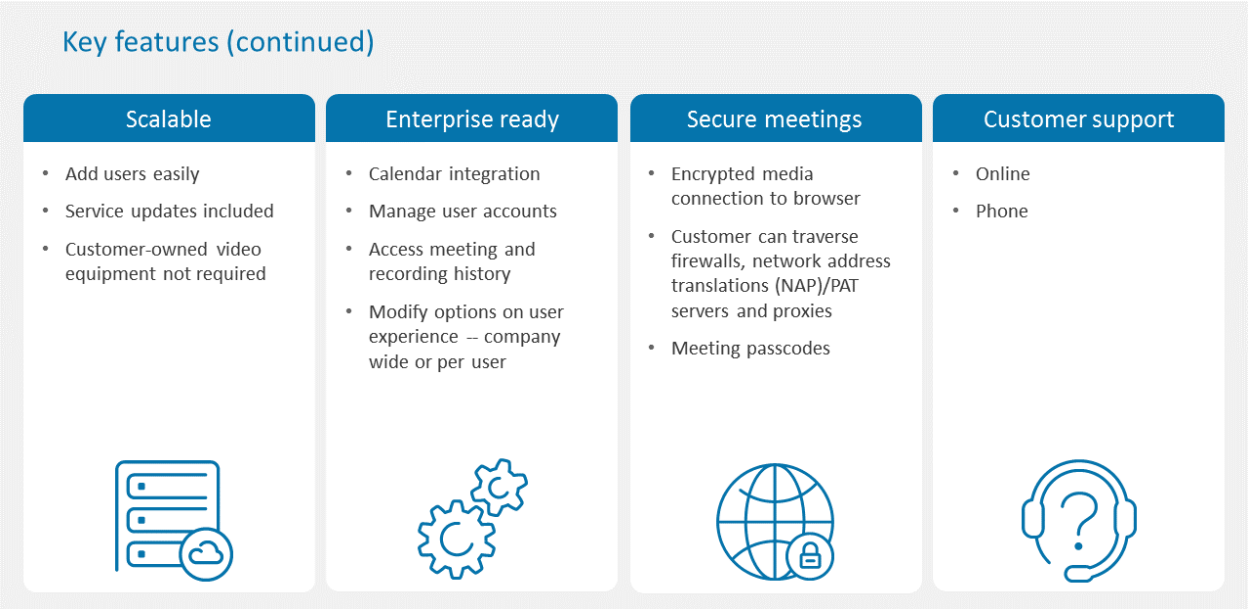
To fulfill the need for a fully integrated video teleconferencing solution our team is proposing AT&T Meetings with BlueJeans. This solution offers a cloud-based video bridging capability that can integrate services like Skype for Business and Google Chat with traditional standards-based room video systems. 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.

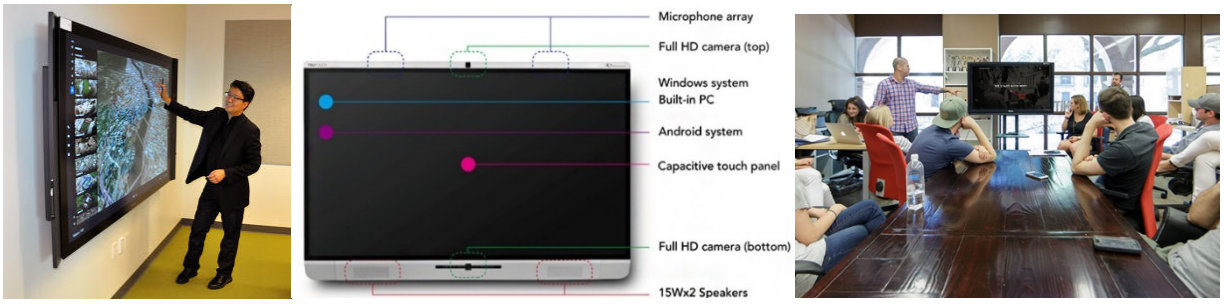
By moving to a Skype for Business standard, all devices and users with access to SfB would be supported, including laptops, desktops, and mobility devices using the SfB client or mobile application. This enables participation and interaction from anywhere, removing the current requirement to have physical 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.

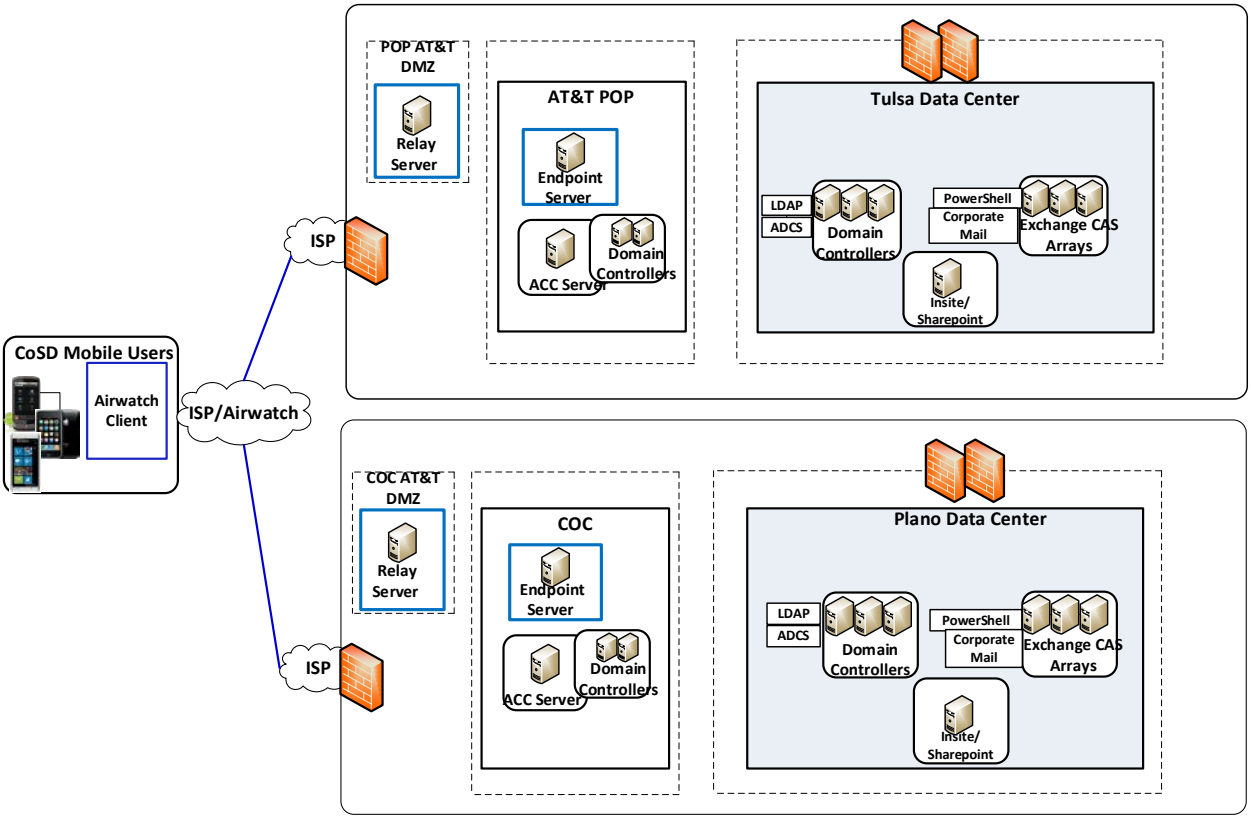
Due to the nature of the cloud service and the geo-redundant configuration of the on premise infrastructure, the AT&T MDM solution has no identified single points of failure.

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.

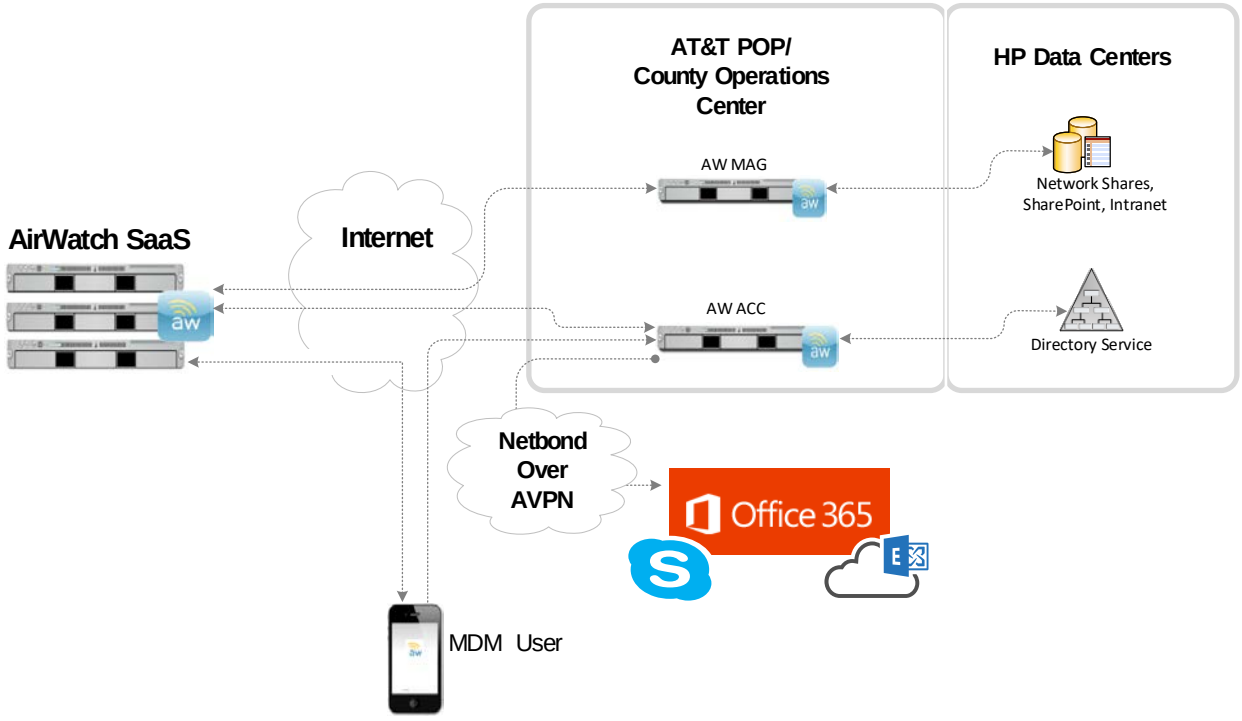
Mobile User and Device Authentication

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

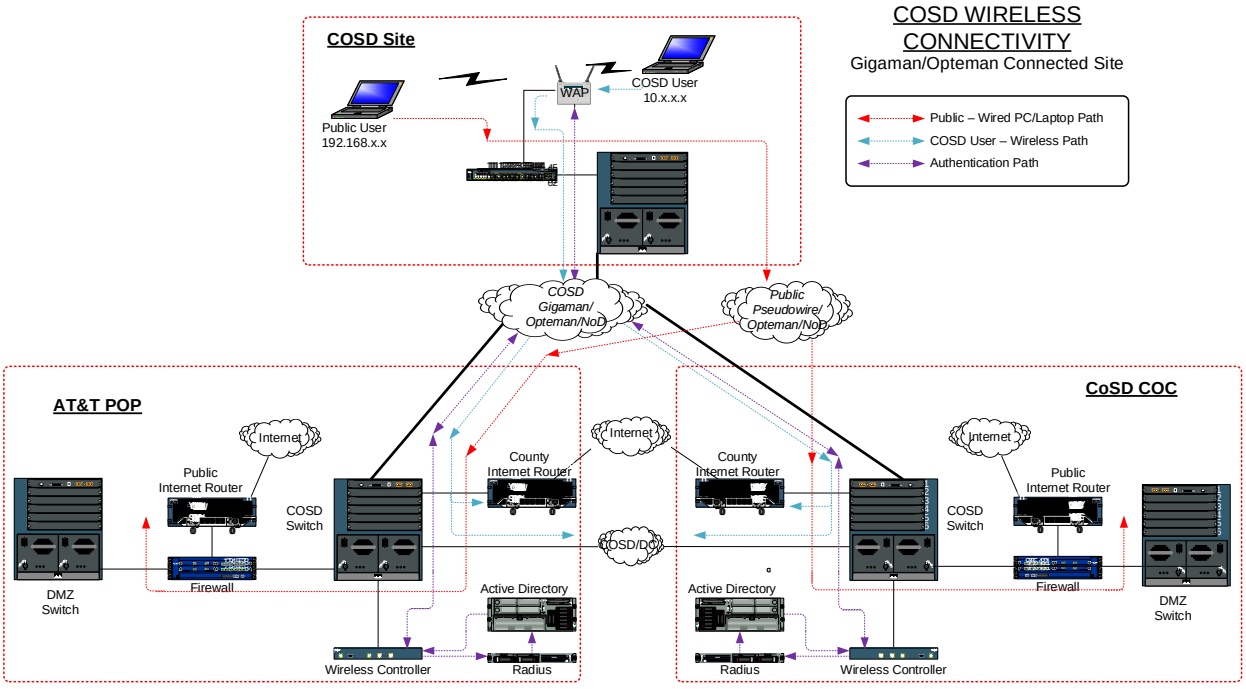
single point of interface for changes and monitoring, and support a variety of access point models. Figure 77 details the County's geo-redundant wireless controller infrastructure.

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

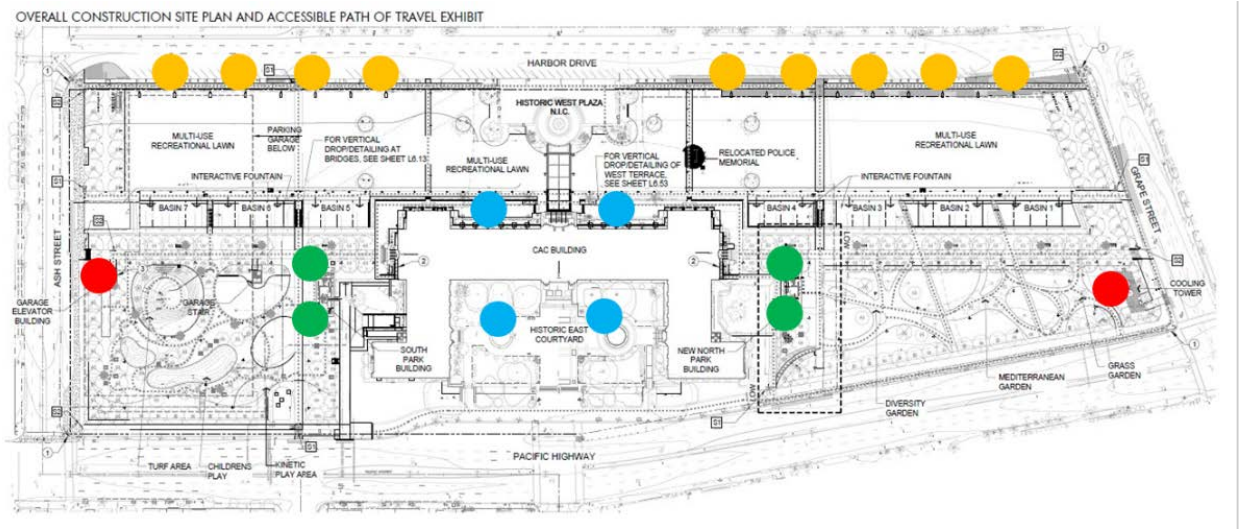
infrastructure, including content filtering functionality, to provide the most robust security available for the wireless infrastructure.

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

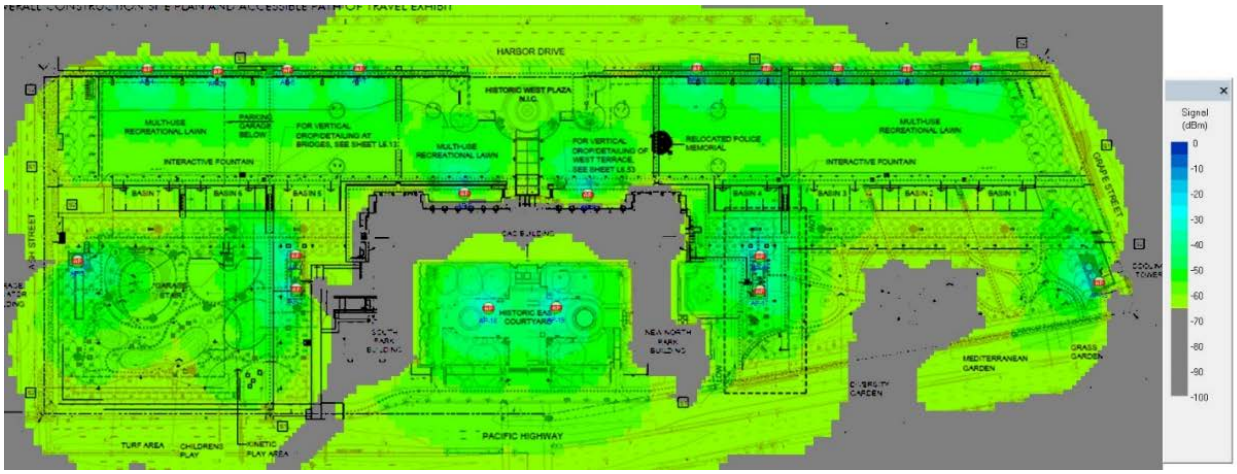
In 2015 our team proactively developed a proposed design for outdoor wireless coverage at the County's Waterfront Park (Figure 78 and Figure 79). This design included an in-depth analysis of the radio frequency (RF) environment to provide a comprehensive and detailed view of the environment and articulate 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.

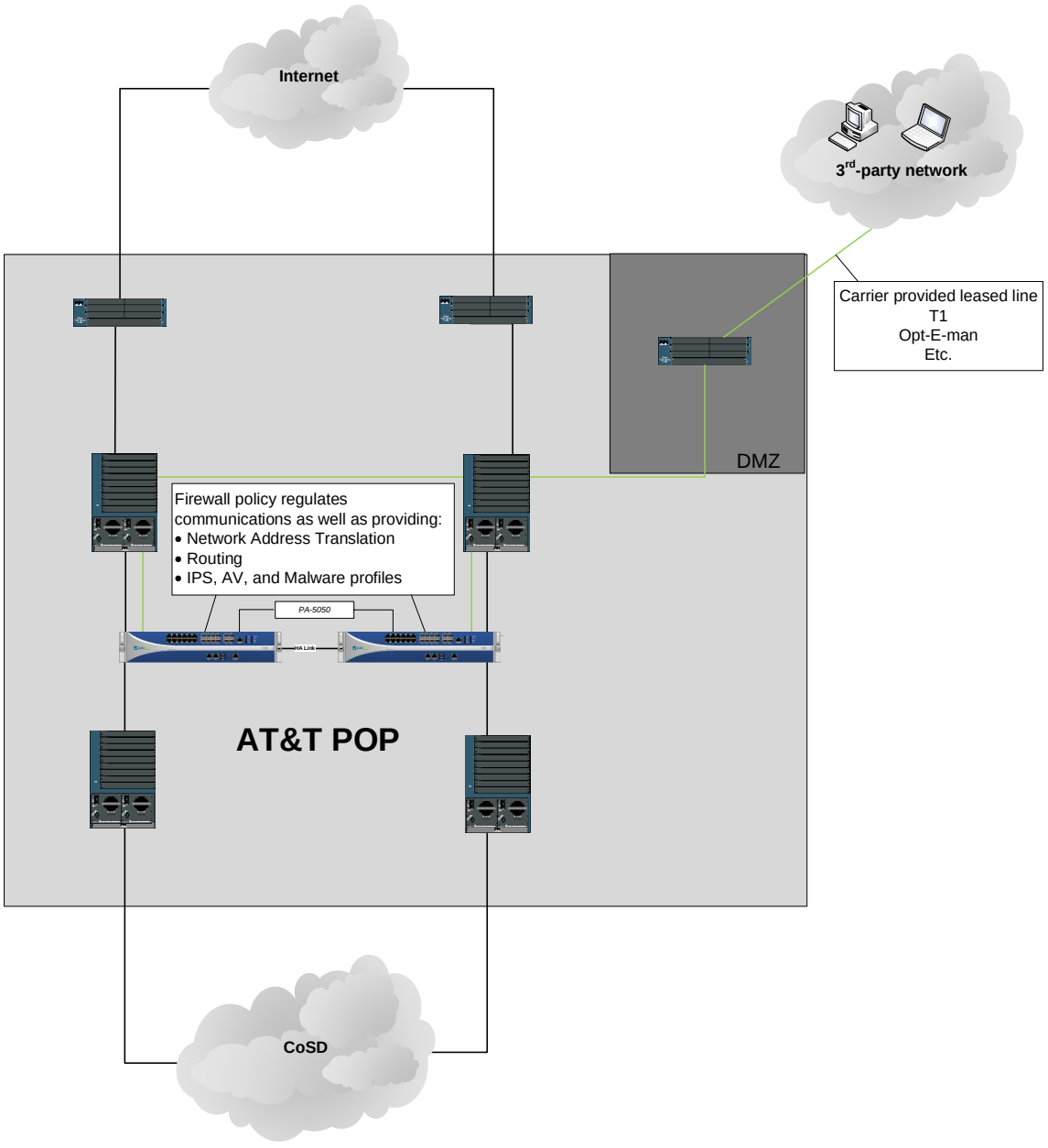
The third-party network access models and use cases are as follows:

- **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.

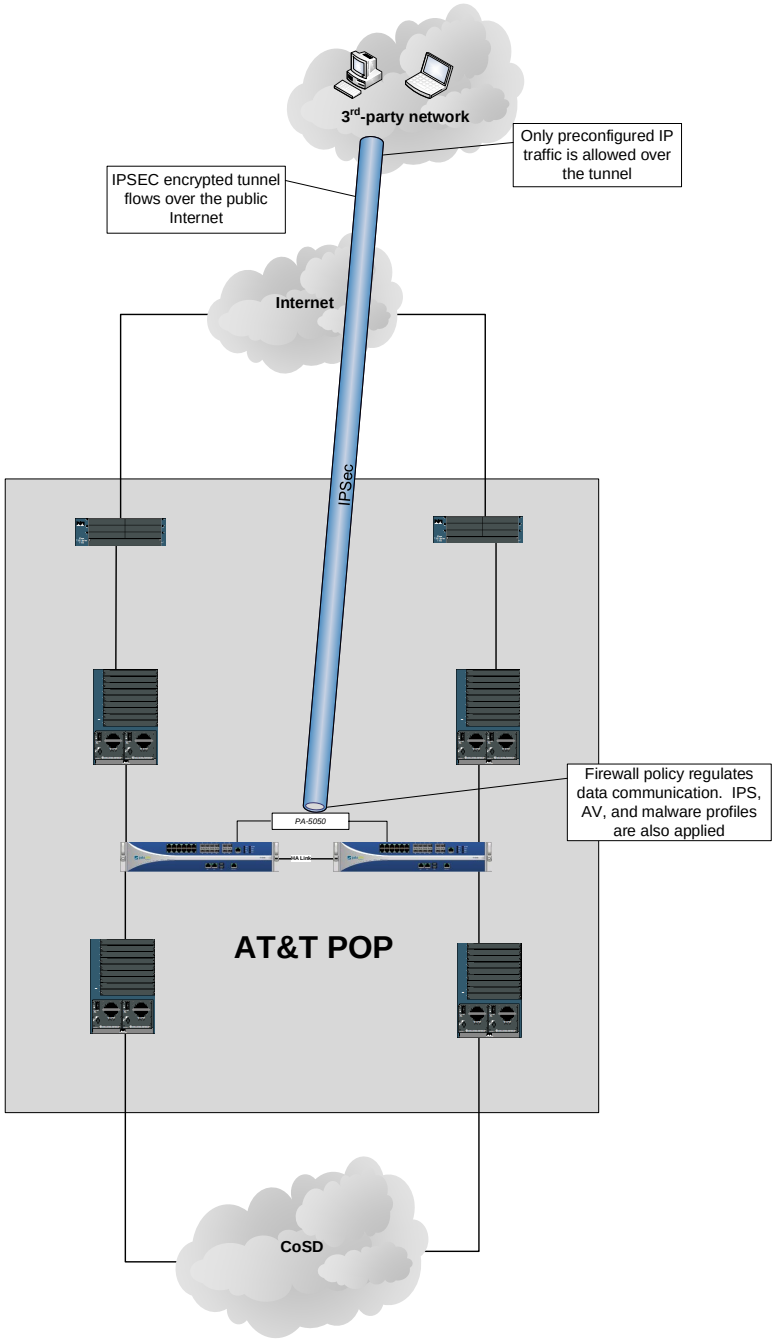
- **Virtual Circuits.** The virtual circuit design allows placement of non-County devices onto the County network in a way that keeps them isolated from County assets. All communication to and from County resources is still regulated by firewall policies. Presently, this solution supports users within 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



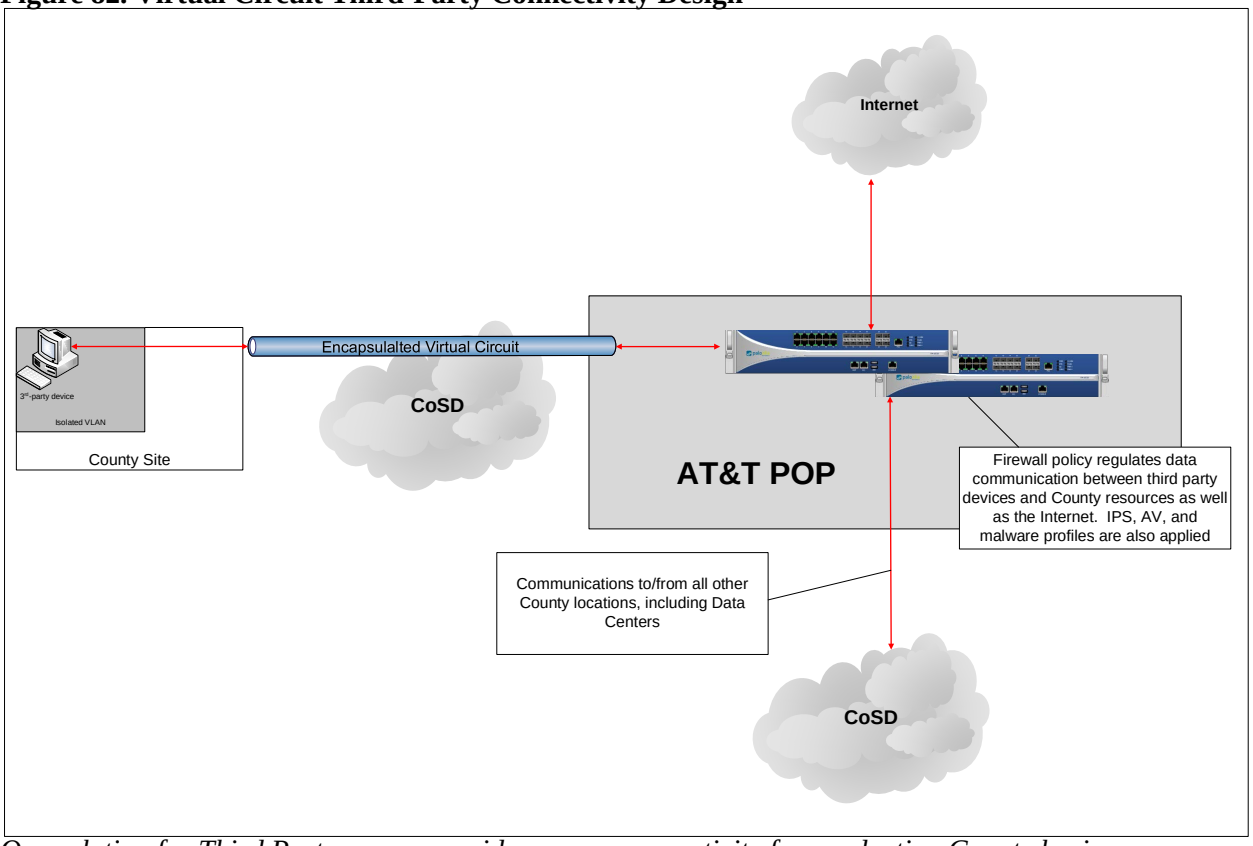
Our solution for Third Party access provides secure connectivity for conducting County business.

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

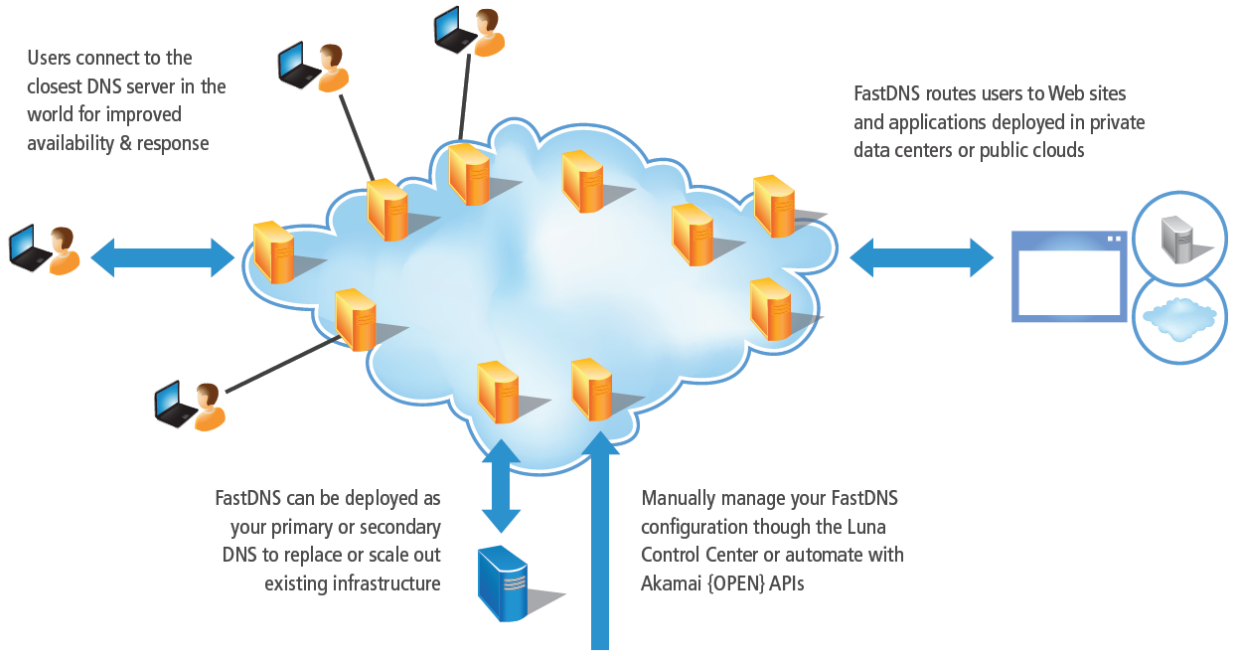
In mid-2015 our team worked with the County to re-architect and migrate external Domain Name Service (DNS) to a scalable, redundant, and fault-tolerant cloud-based platform. This recently implemented solution, using Akamai cloud-based FastDNS service, will be the basis for our DNS management service 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.

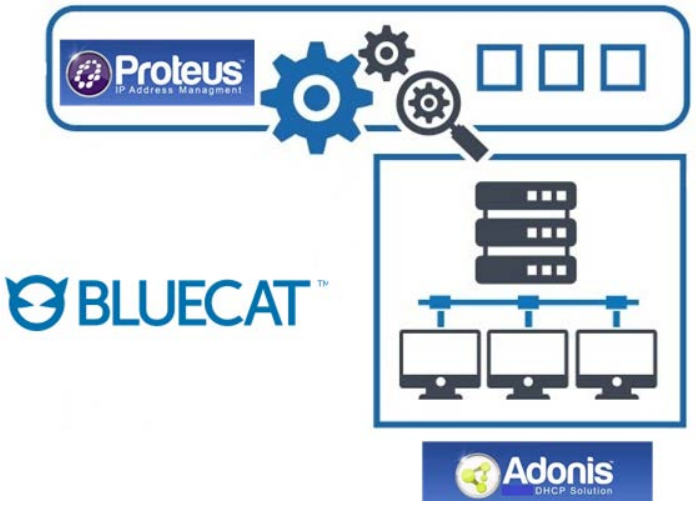
None.

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

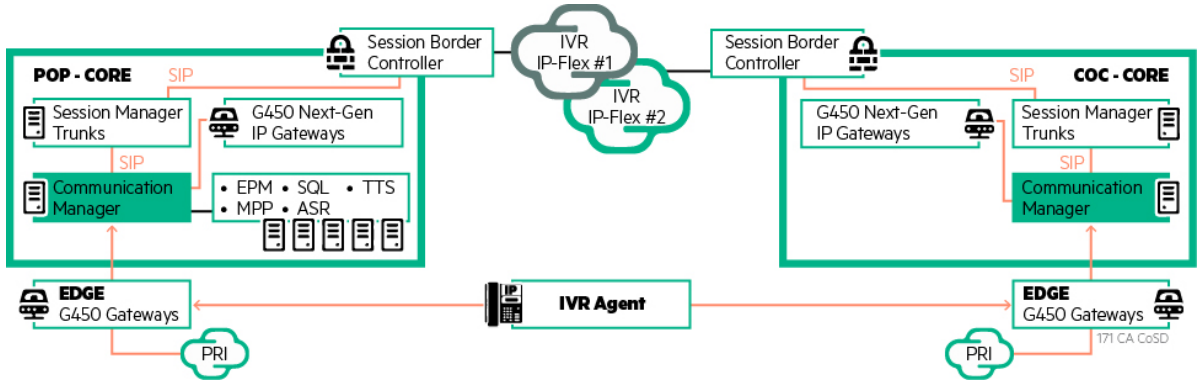
Integrated Voice Response

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:

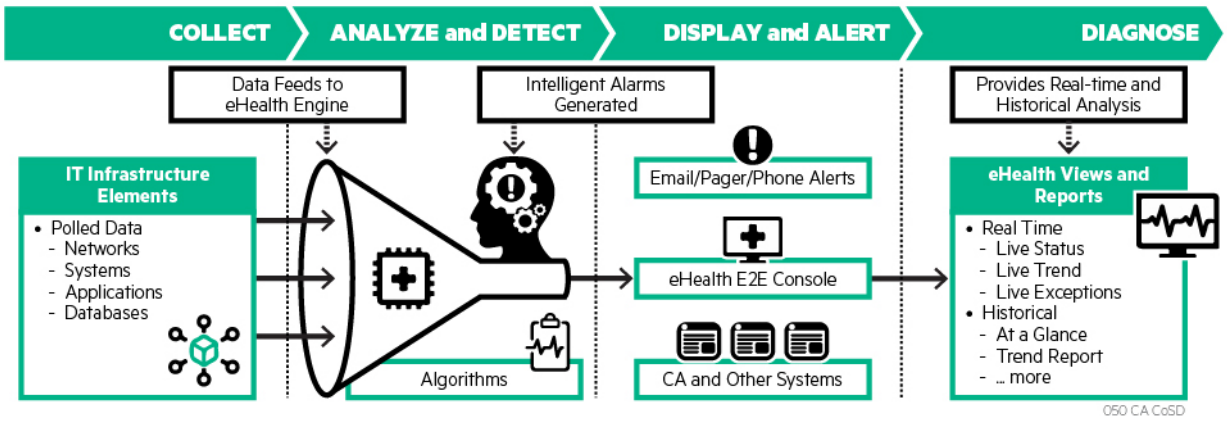
- Network bandwidth monitoring to specified thresholds
- CPU/memory utilization and errors monitoring on all network devices to specified thresholds
- Responsive impact assessment and mitigation planning
- Proactive trend-based "situational watch list" assessments and corresponding action plans
- Real-time 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.

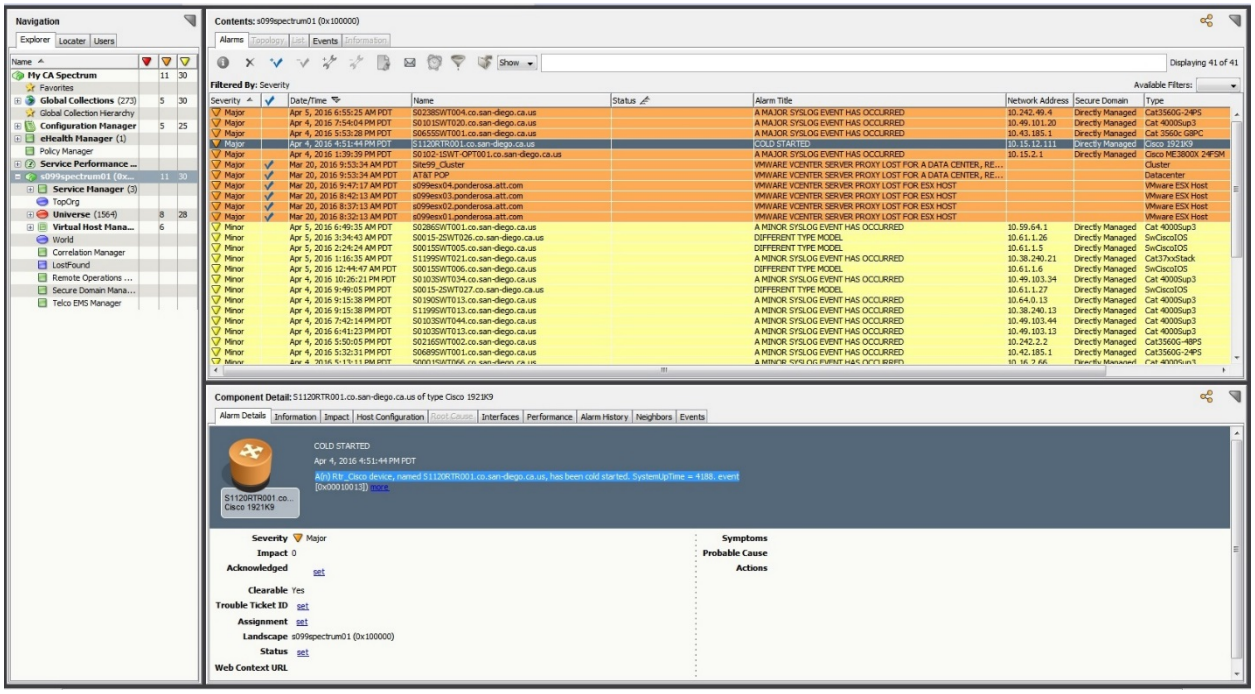
Threshold severity is currently defined in four levels, each dictating an appropriate course of action as listed in Table 53.

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



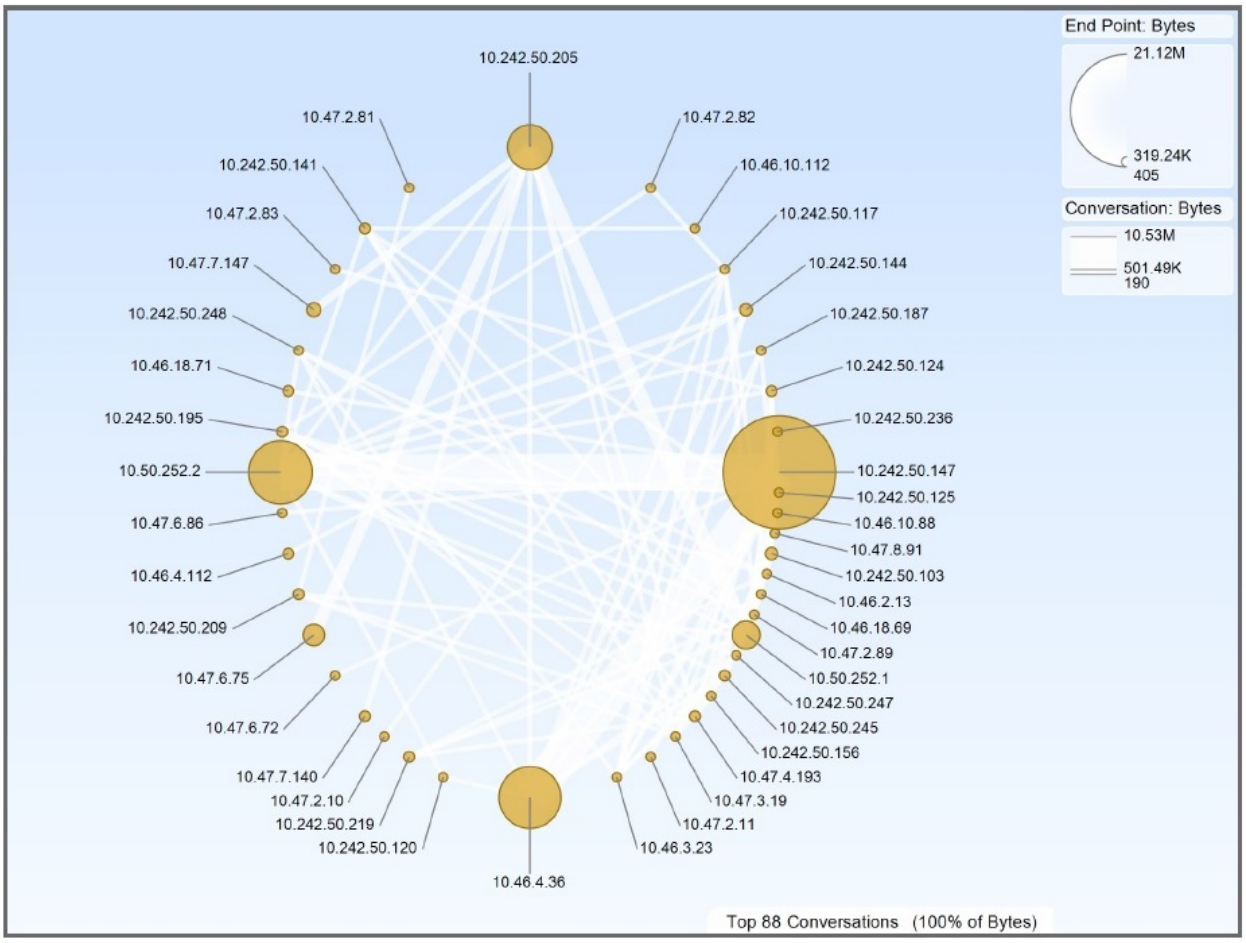
CA Spectrum's Threshold Alarming function provides real-time view into various alarm categories, with the ability to drill down on each event.

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

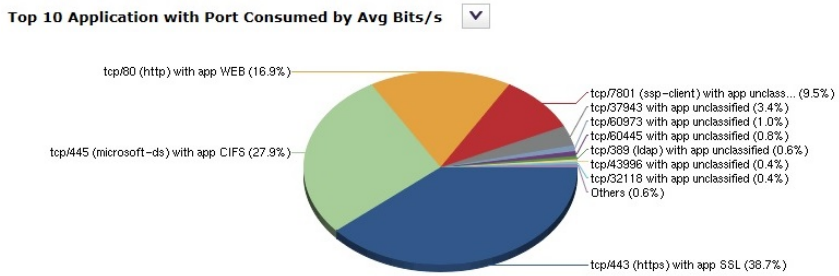


The Riverbed Cascade tool is able to identify traffic patterns across the enterprise, allowing for drill down on specific network segments.

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

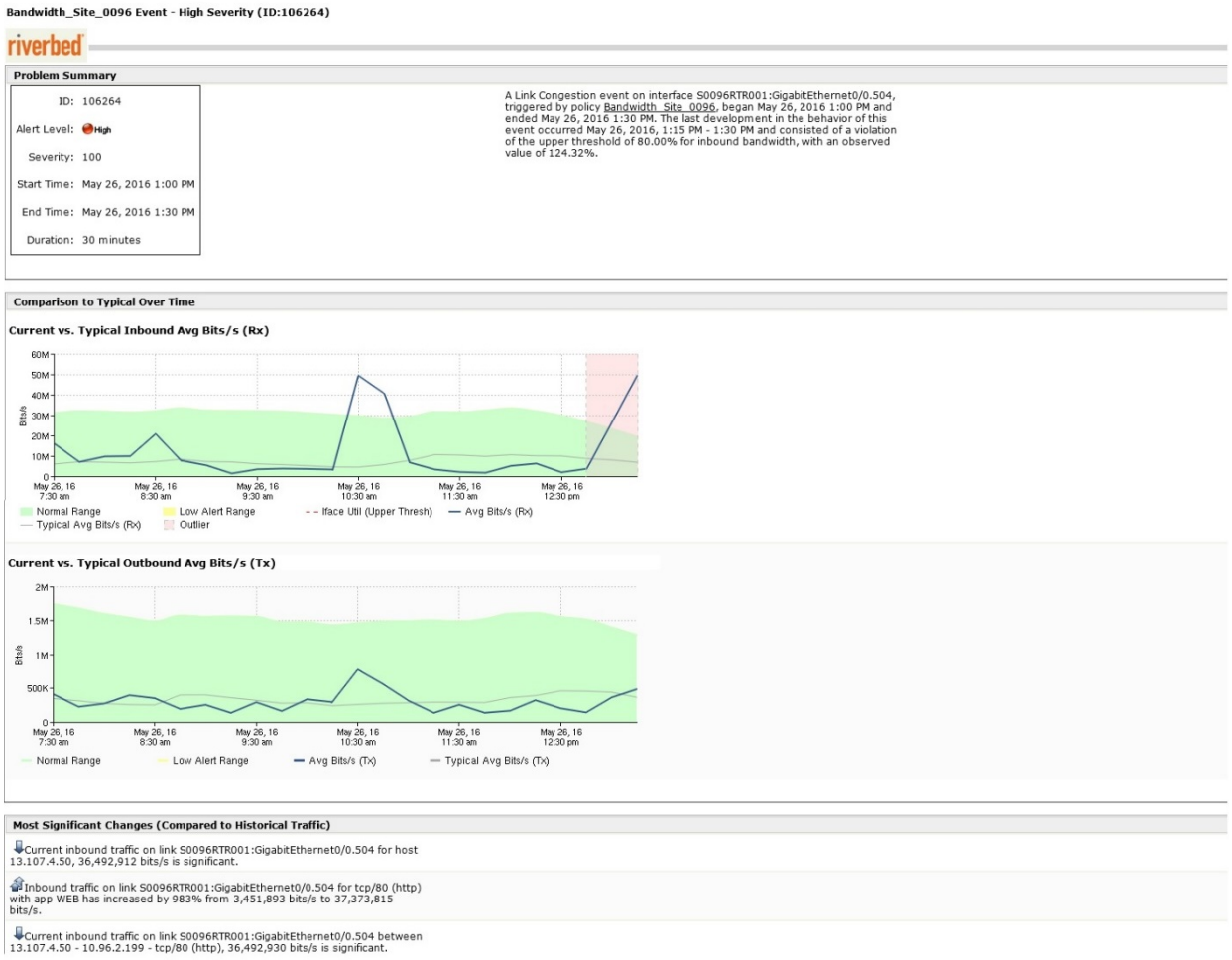
The Riverbed Cascade tool's deep packet analysis capability provides specific application level detail, used in forensic and real-time anomaly detection.

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.

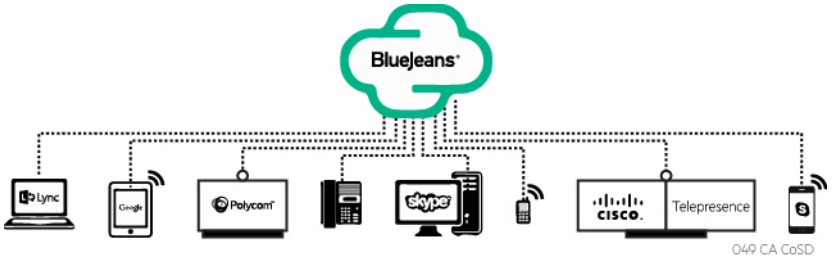
The members of this team will be identified by each framework as responsible for performance management in their discipline and will dedicate the necessary time to maintain a best in class performance analytics function. By taking early action, this team will drive through chronic issues and eventually 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.

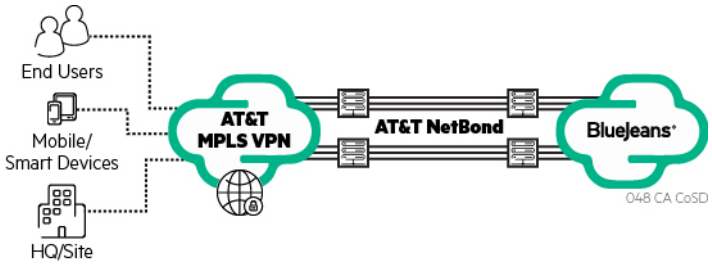
Figure 91. AT&T Meetings with BlueJeans



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.

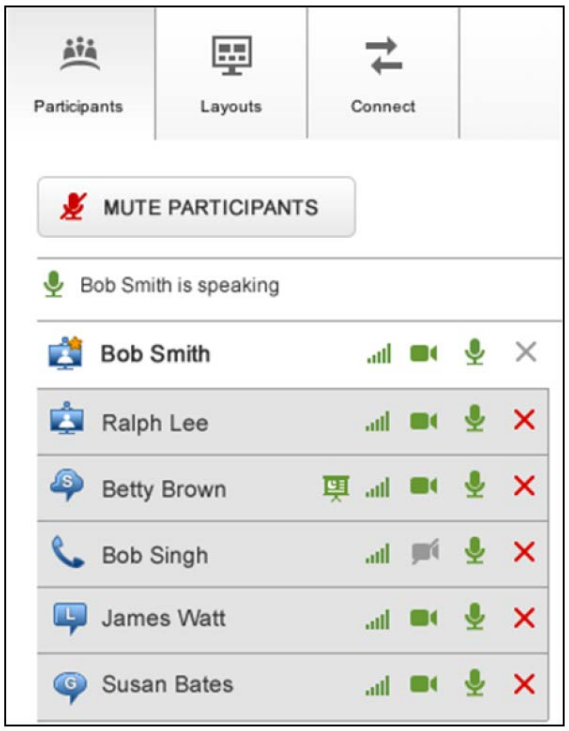
Figure 93. BlueJeans Conferencing Solution



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.

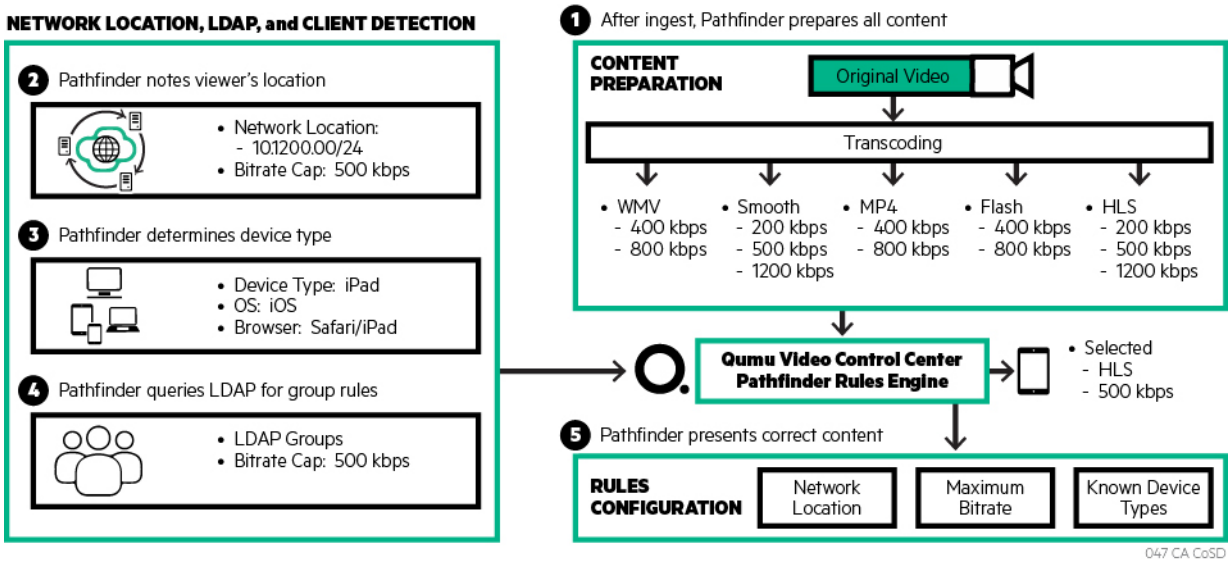
After analyzing these provider options, HPES recommends AT&T Video Management Services (AVMS) to provide town hall video services for the County. AT&T and its partner Qumu are uniquely positioned in the industry to deliver high quality live and video on demand services. Qumu is ranked within the upper 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.

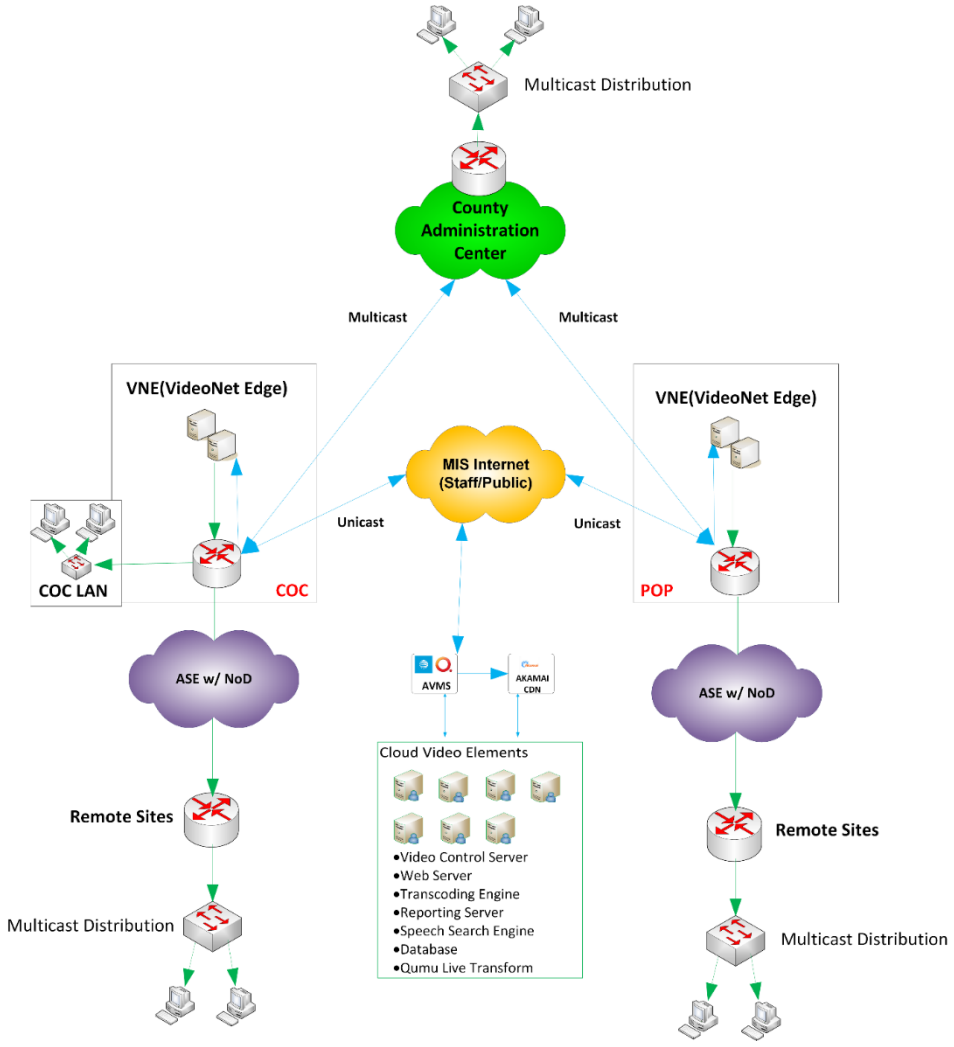
Embedded polling and feedback features offer increased benefit to the County by engaging viewers and soliciting their input. High grade analytics will provide viewer statistics along with broadcast performance detail to provide a clear picture of content performance and identification of possible impacts.

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.

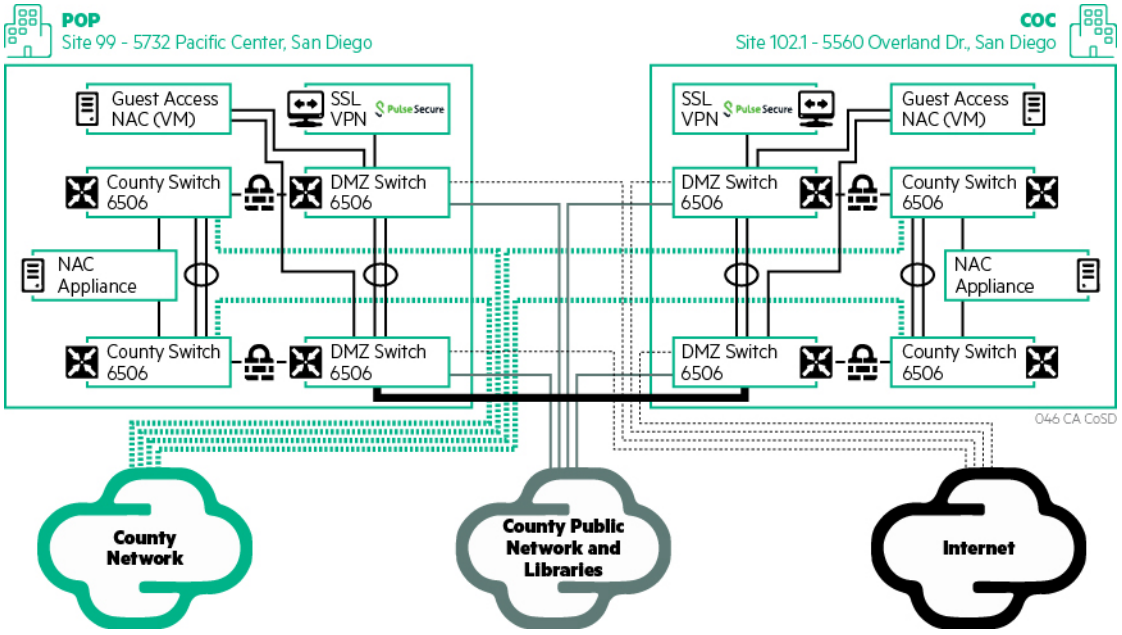
Video is the future of corporate communications, as evidenced by its extensive use in the private sector by large fortune 50 companies. With an enterprise the size of the County of San Diego, the opportunities that this technology represents are extensive. The AVMS solution proposed by the HPES team 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.

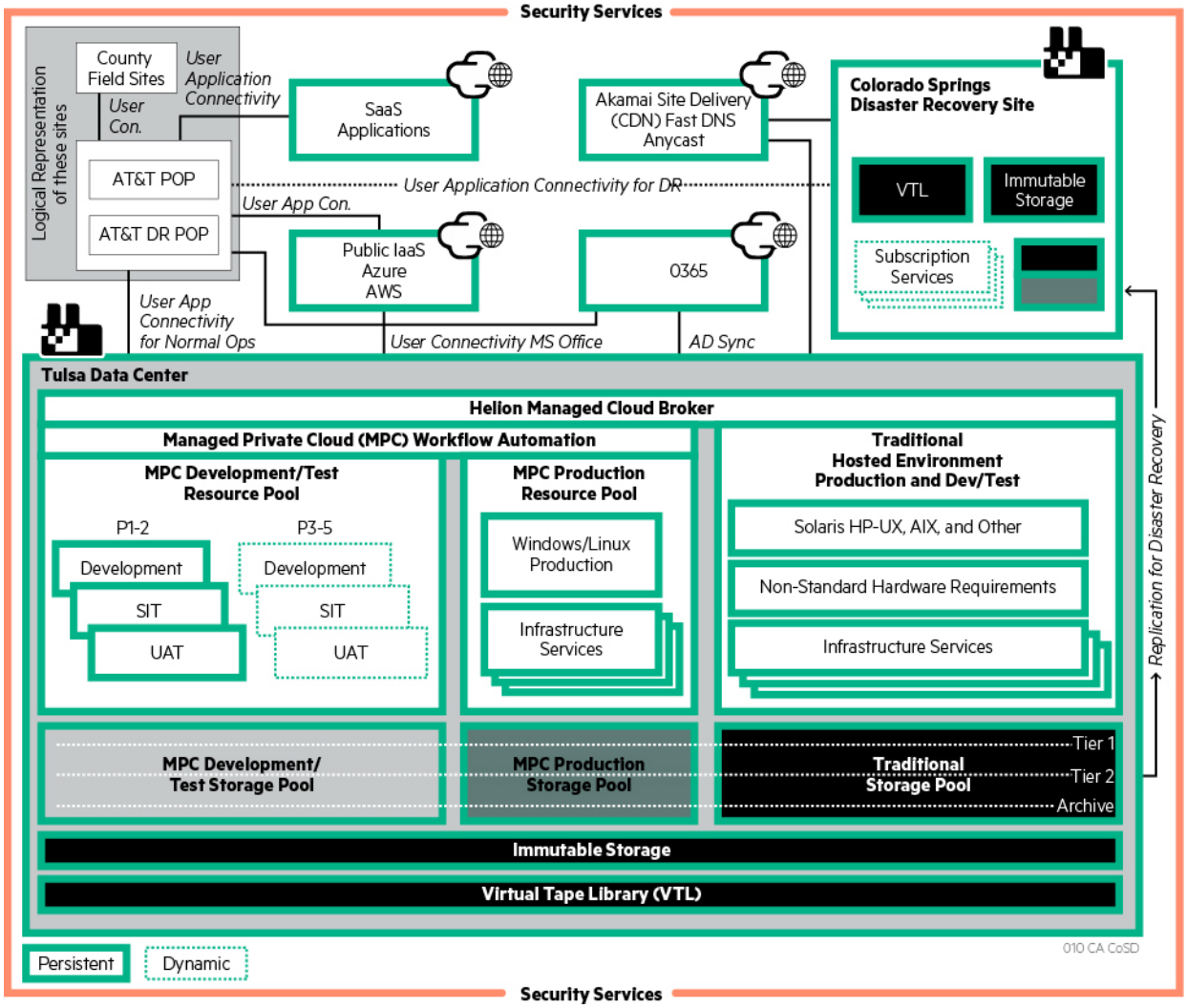
HPES has demonstrated our commitment to the ongoing transformation of the County's network. The model for local Government IT outsourcing was pioneered by the County, with HPES as a trusted advisor in every engagement since its inception. We can continue to apply our experience, vision, and knowledge 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

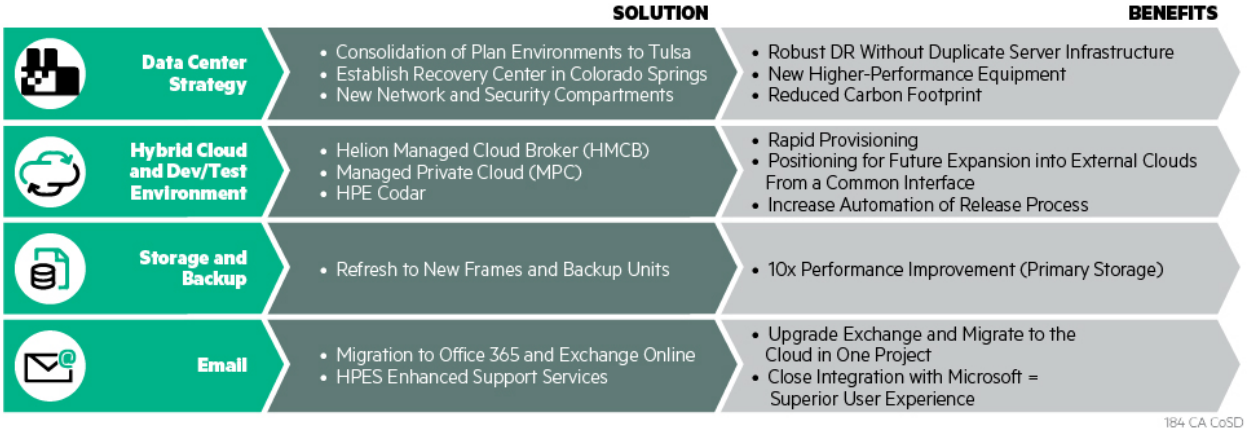


HPES' robust data center services framework solution will meet the County's needs and requirements to consolidate data center services in Tulsa.

Framework Components

The proposed data center strategy and its benefits are summarized in Figure 100.

Figure 100. Data Center Solution Key Benefits

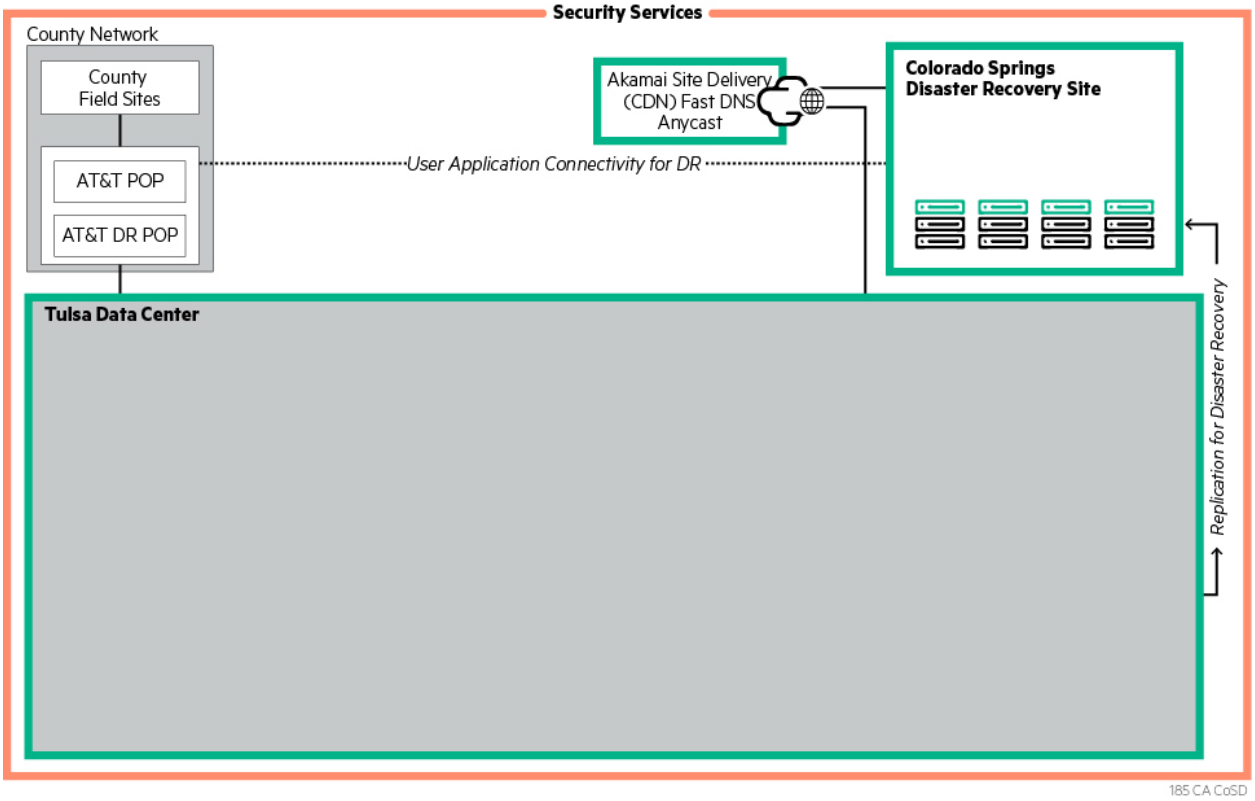


Our Data Center Framework strategy positions the County for the next wave of IT services as well as making some of those services a reality right away.

- 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



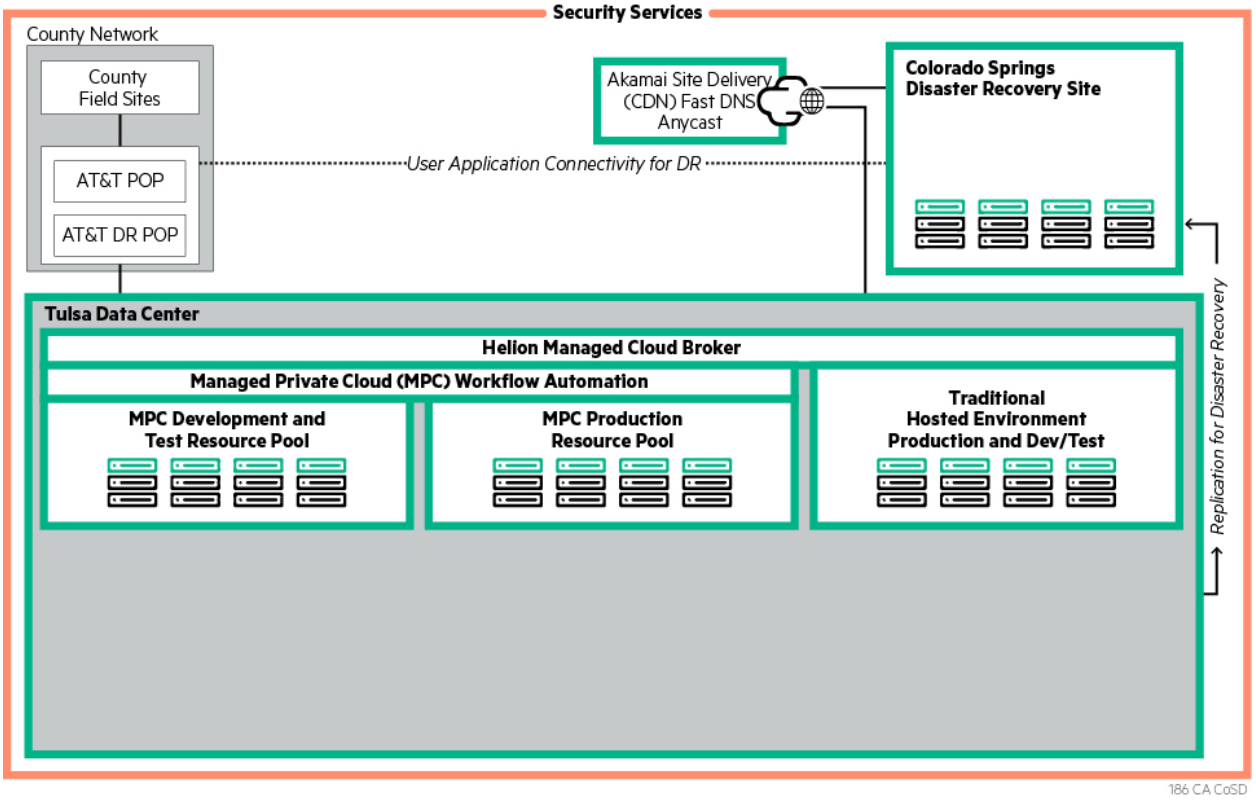
Two primary sites are no longer required for rapid recovery: our solution provides a consolidated site and a highly flexible and secure Disaster Recovery site.

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



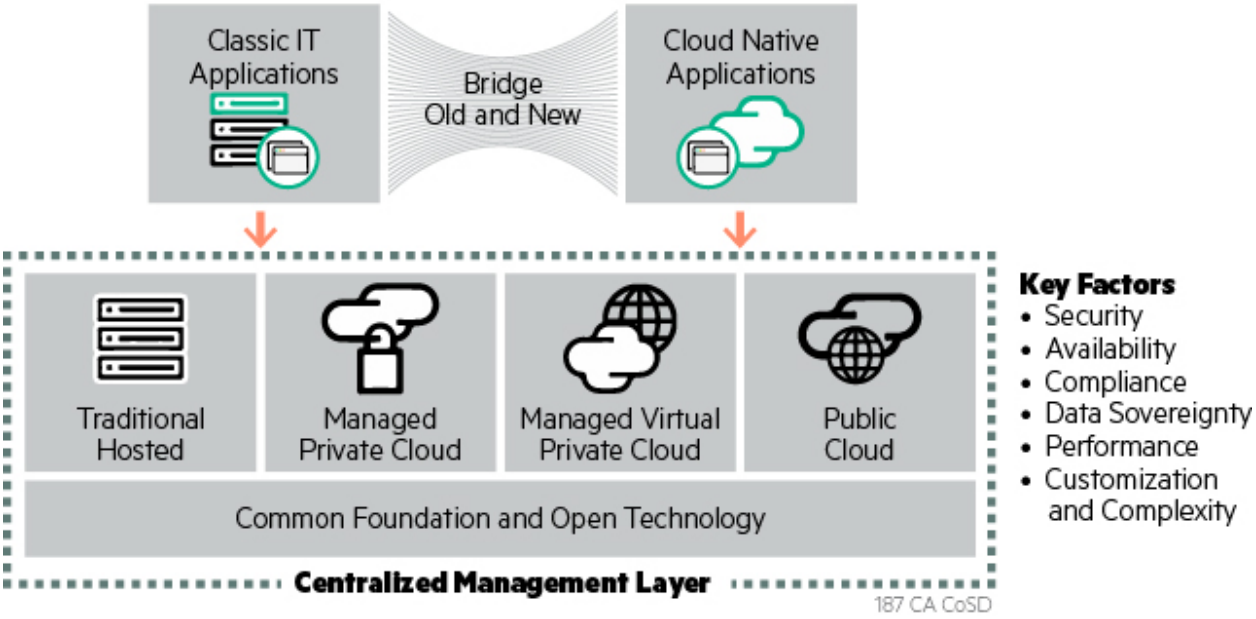
The Hybrid Cloud solution provides extensibility into future cloud services while making some of the benefits of cloud services available today.

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.

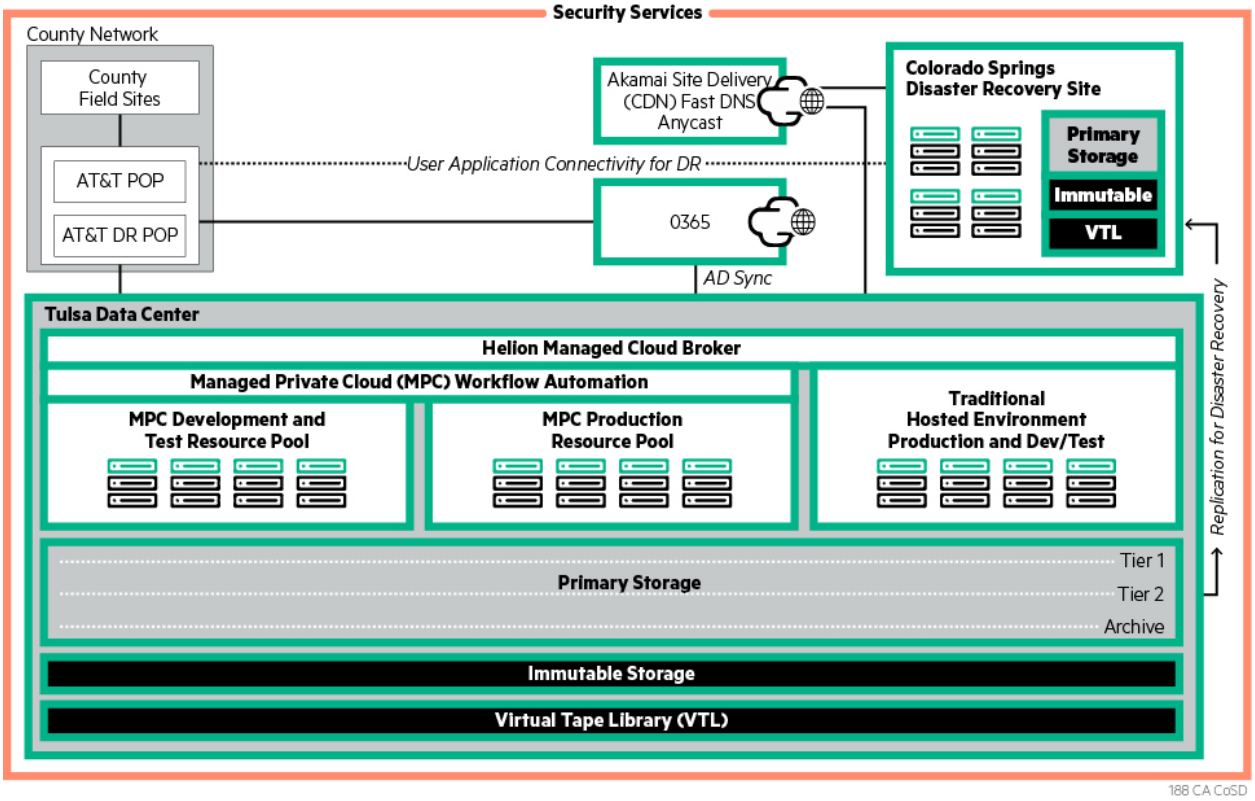
The factors shown above illustrate the drivers for choosing one type of environment over another. Higher levels of security, customization, complexity, etc., are factors that would likely favor the Traditional Hosted side of the spectrum. "Cloud native" applications are, by nature, more encapsulated 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.

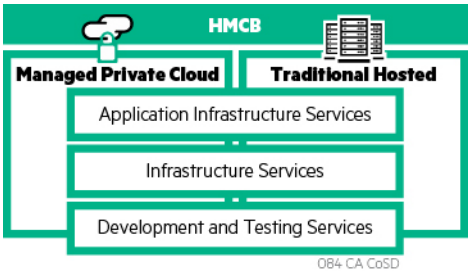
Application Infrastructure Services (Sched. 4.3, Section 6.7)

- 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

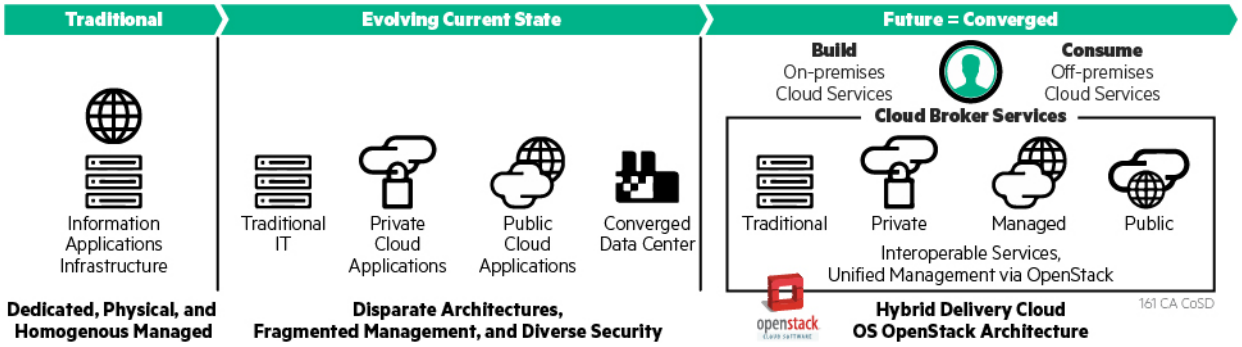
- Supplying standard consumption reports

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).

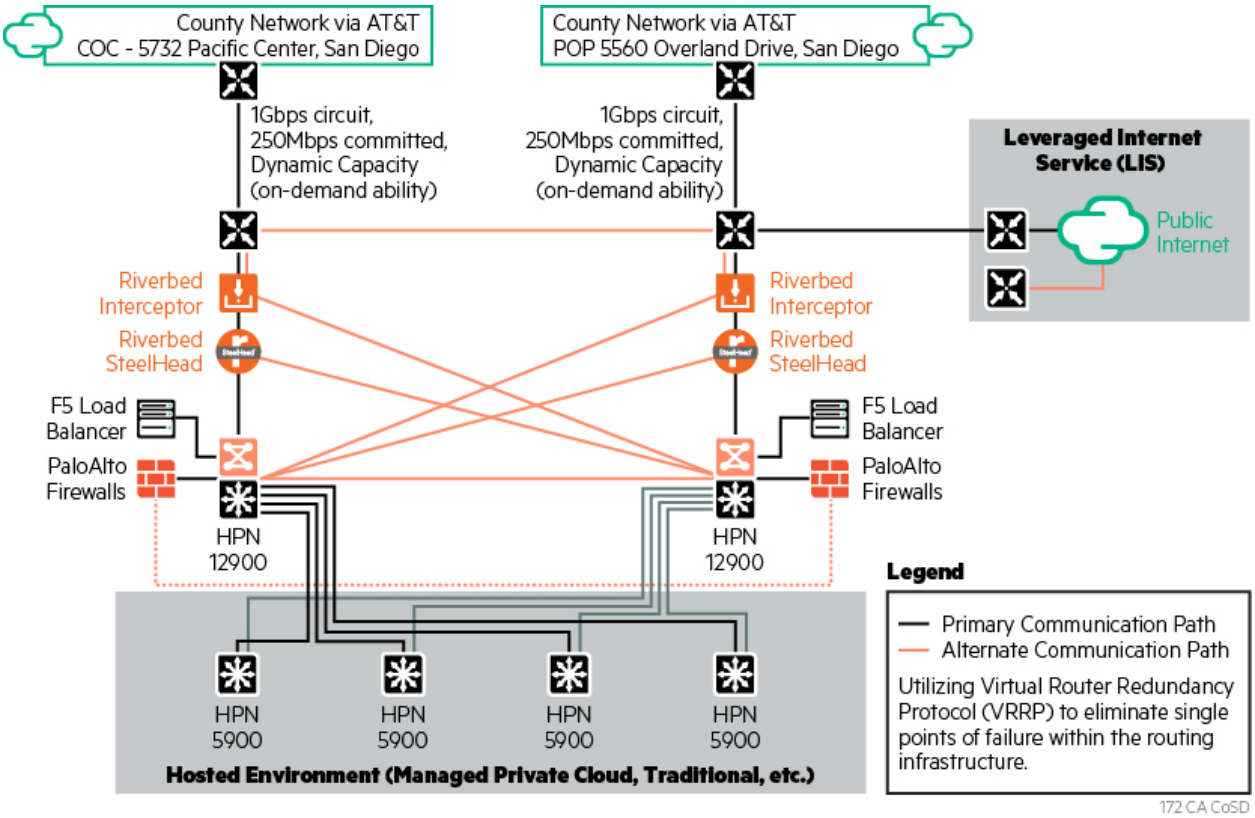
Backup and Restore Services—Backup services for virtual and physical computing services, provide operating system and filesystem (offline) backup for computing services to enable data restoration after a data loss event. Backups are accomplished by copying the specific data to backup media. We will perform 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.

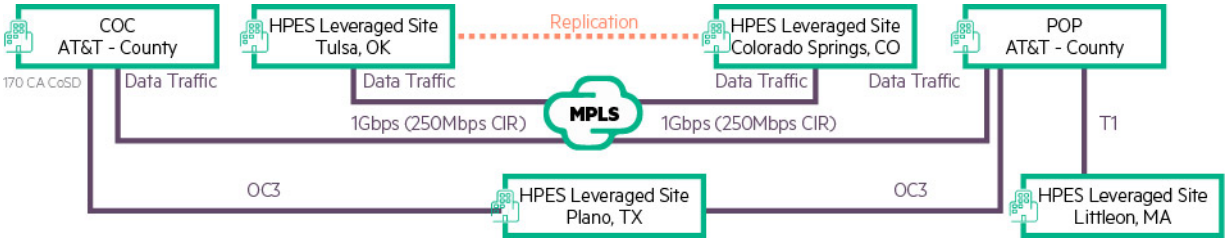
Figure 108. Data Center Network Detail



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.

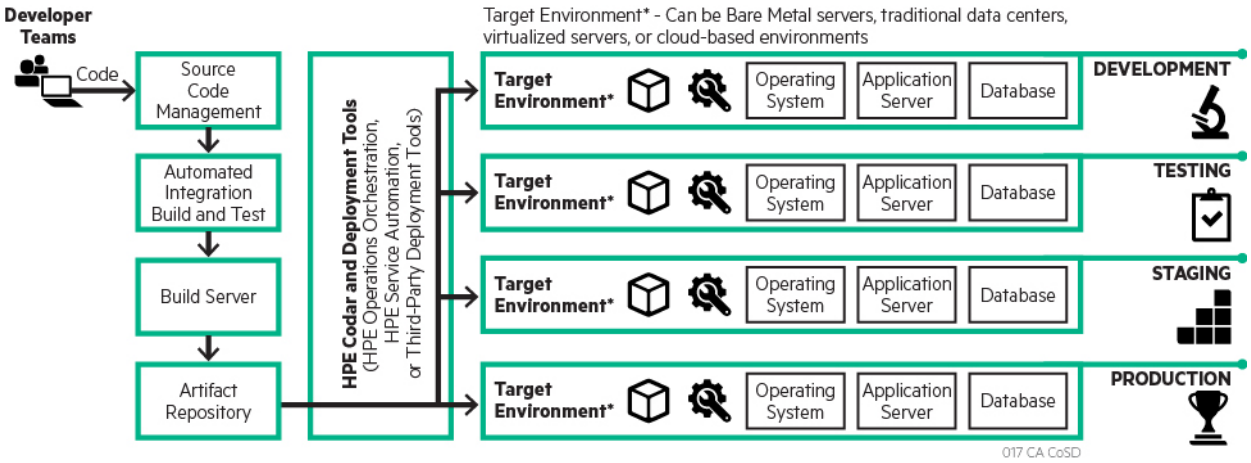
The Dev/Test environment is designed to meet County goals for continual improvement and cost effective innovative services to help the County transition to a marketplace of hybrid-provided services governed by Reports 49/50 standards and County IT strategy. Financial governance of the Dev/Test environment 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.

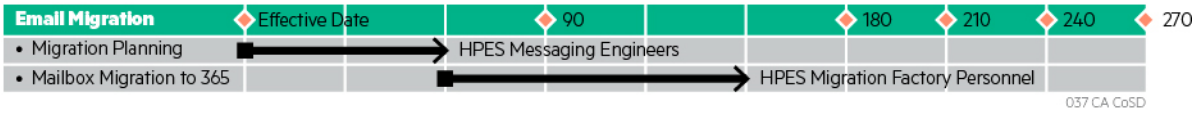
WacViewingOnPublicComputersEnabled	Specifies whether a user who has signed into Outlook Web App from a computer outside of the corporate network can view supported Office files using Outlook Web App.
WacViewingOnPrivateComputersEnabled	
WebReadyDocumentViewingOnPublic ComputersEnabled	
WebReadyDocumentViewingOnPrivate 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

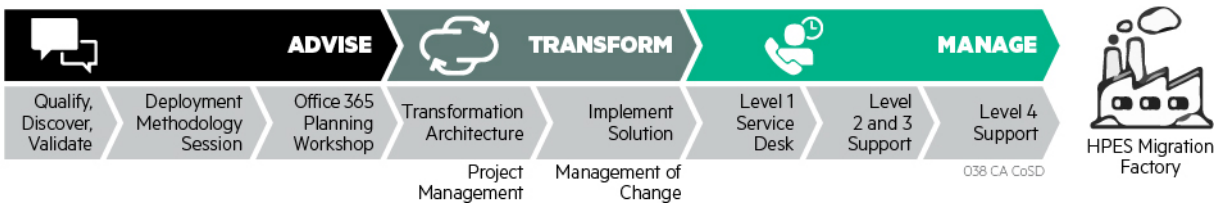
Roles or tasks	HPES	Microsoft
HPES and Microsoft Office 365 support team	– HPES presence in Microsoft Redmond office – Shared document repository – Knowledge databases, process documents, issue tracking – Weekly team meetings to review tickets, ongoing issues, planned changes, process improvements	
Office 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.

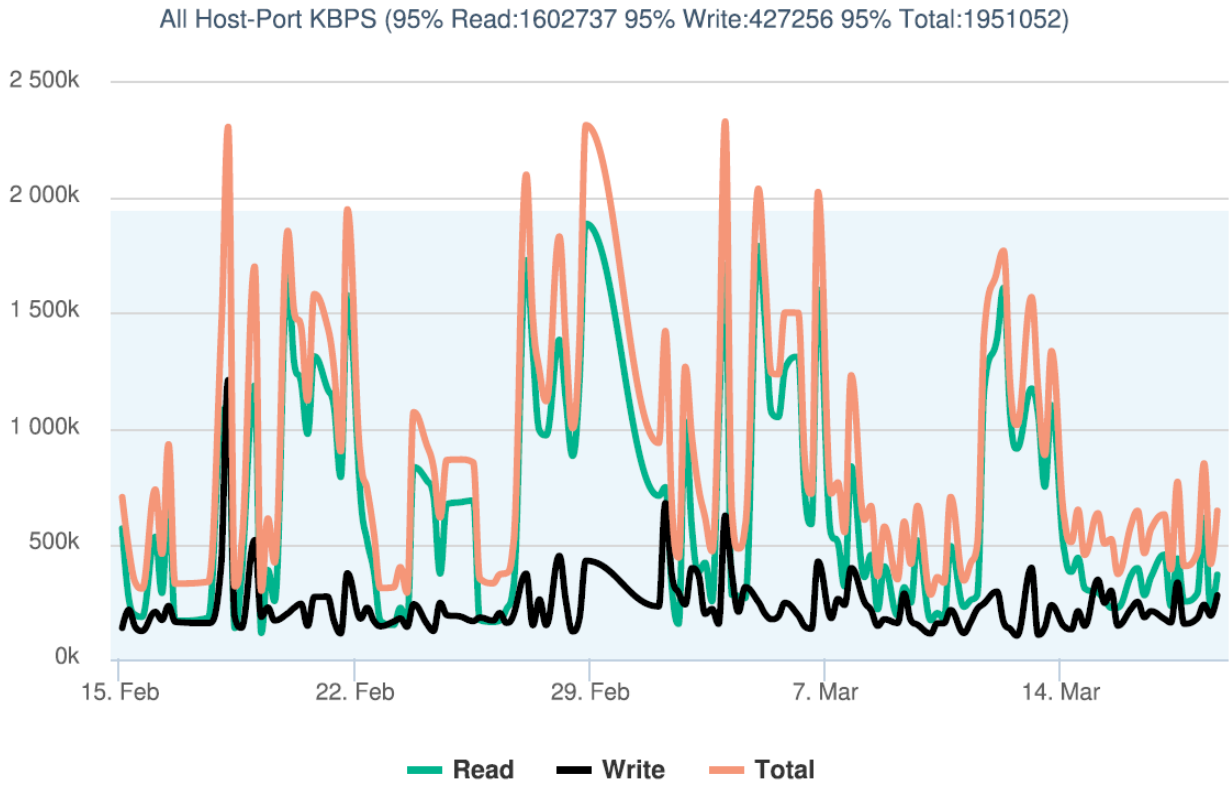
The storage solution provided is a 3PAR 20000 with the same storage tiers provided from 10,000 RPM drives and 7,200 RPM instead of the 15,000 RPM and 7,200 RPM drives. This is possible because the new 3PAR 20000 uses an internal infrastructure to achieve better performance using 10,000 RPM drives. The 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.

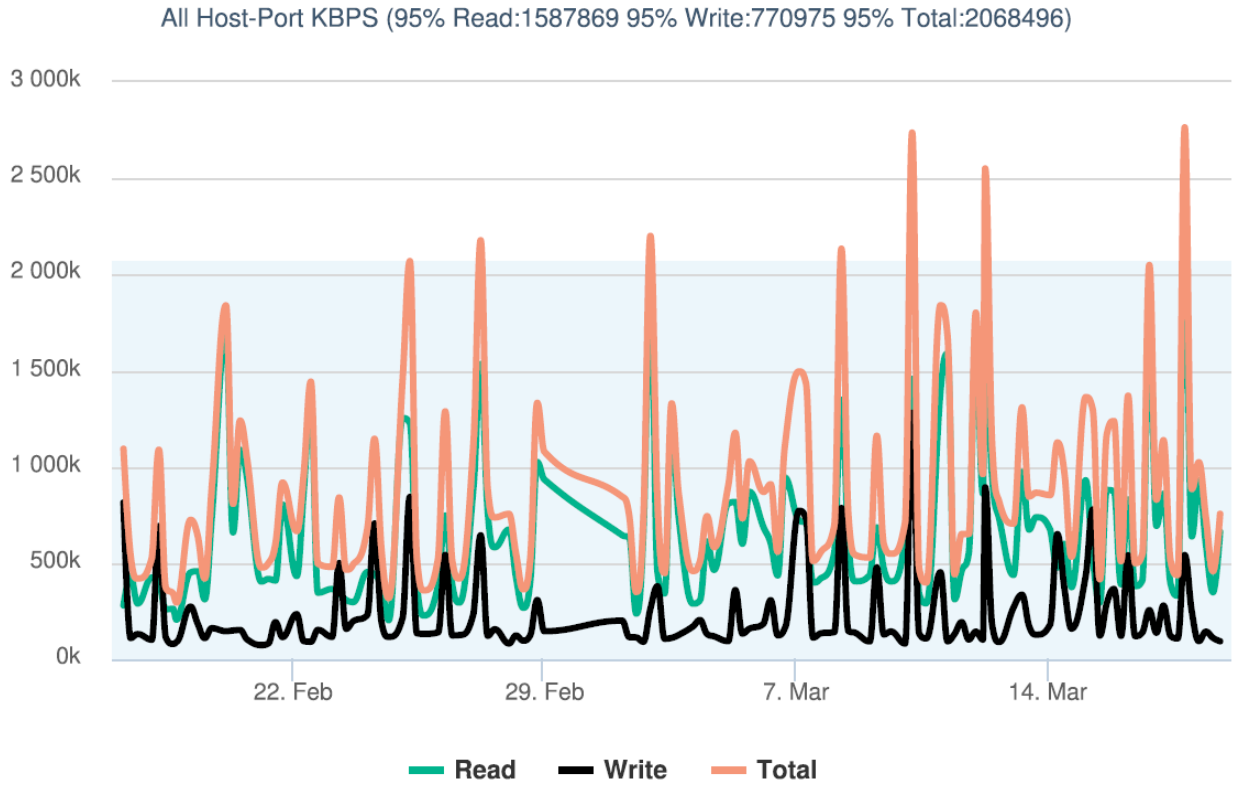
Figure 113. (Tulsa) and Figure 114. (Plano) were generated from the County's recent storage activity. Performance data from the two current 3PARs were used to simulate the expected performance of the new frame. The current Tulsa and Plano 3PAR P10000 reached a peak of ~2450 KBs per second, while the 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.

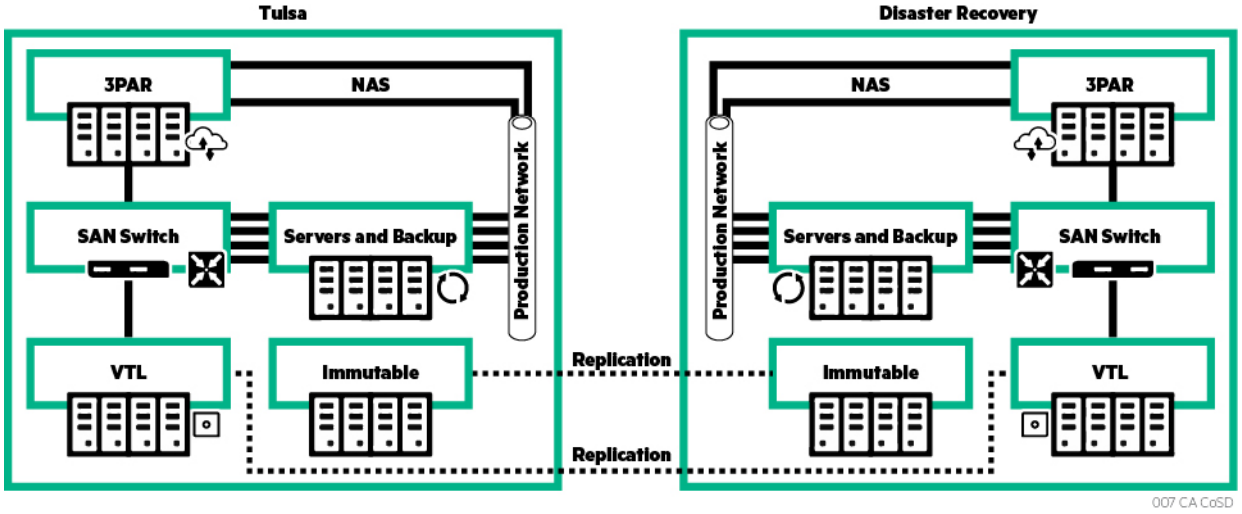
The existing production backup sets will be copied to the new solution so that no backup set data is lost during transition. A StoreOnce VTLat the DR site will join the backup environment as a replication target. Backups will be replicated to the DR site. Full replication of backups serves two purposes:

- 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.

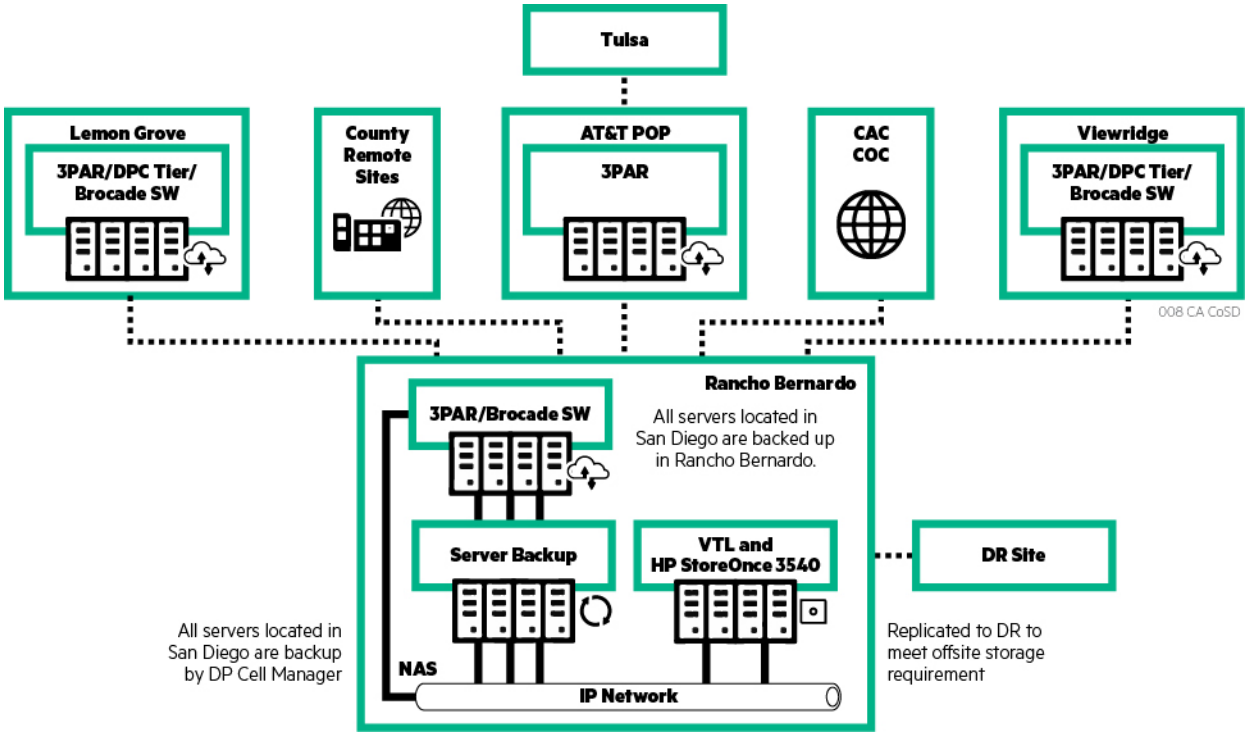
Figure 116. Future Logical View of Data Center Mid-range Server Storage / BUR



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.

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.

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."

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

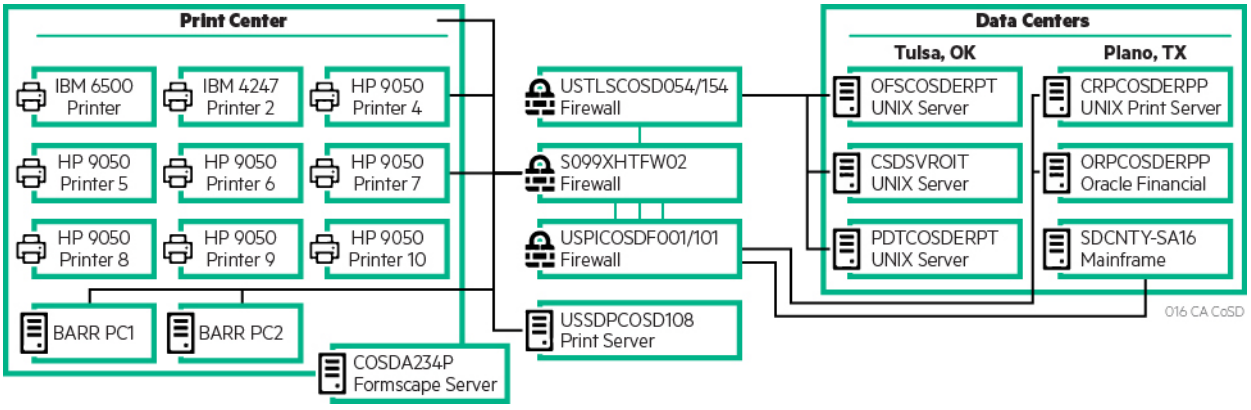
Processes section to facilitate timely and consistent report production and delivery to multiple agencies throughout the County.

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

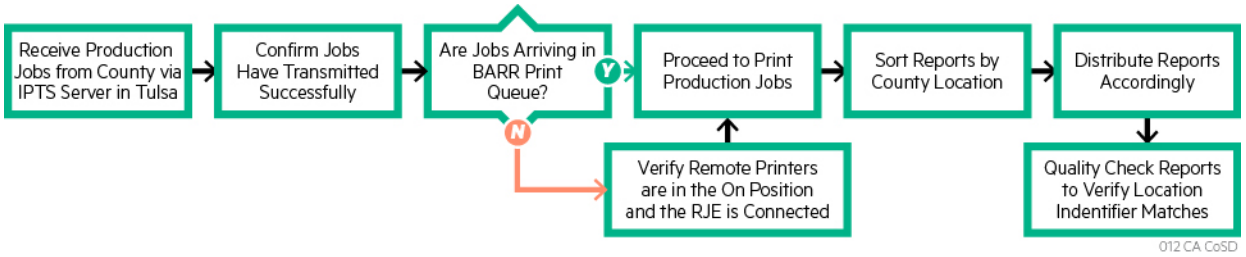
TYPE OF PRINTING	LOCATION
Laser and Impact Print	Rancho Bernardo
Annual tax bills, supplemental (small volume) tax bills, and tax bills that require manual intervention of the Treasurer-Tax Collector's (TTC) office.	Rancho Bernardo, with backup at Rancho Cordova
One-stop document and tax bill management—folding, 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.

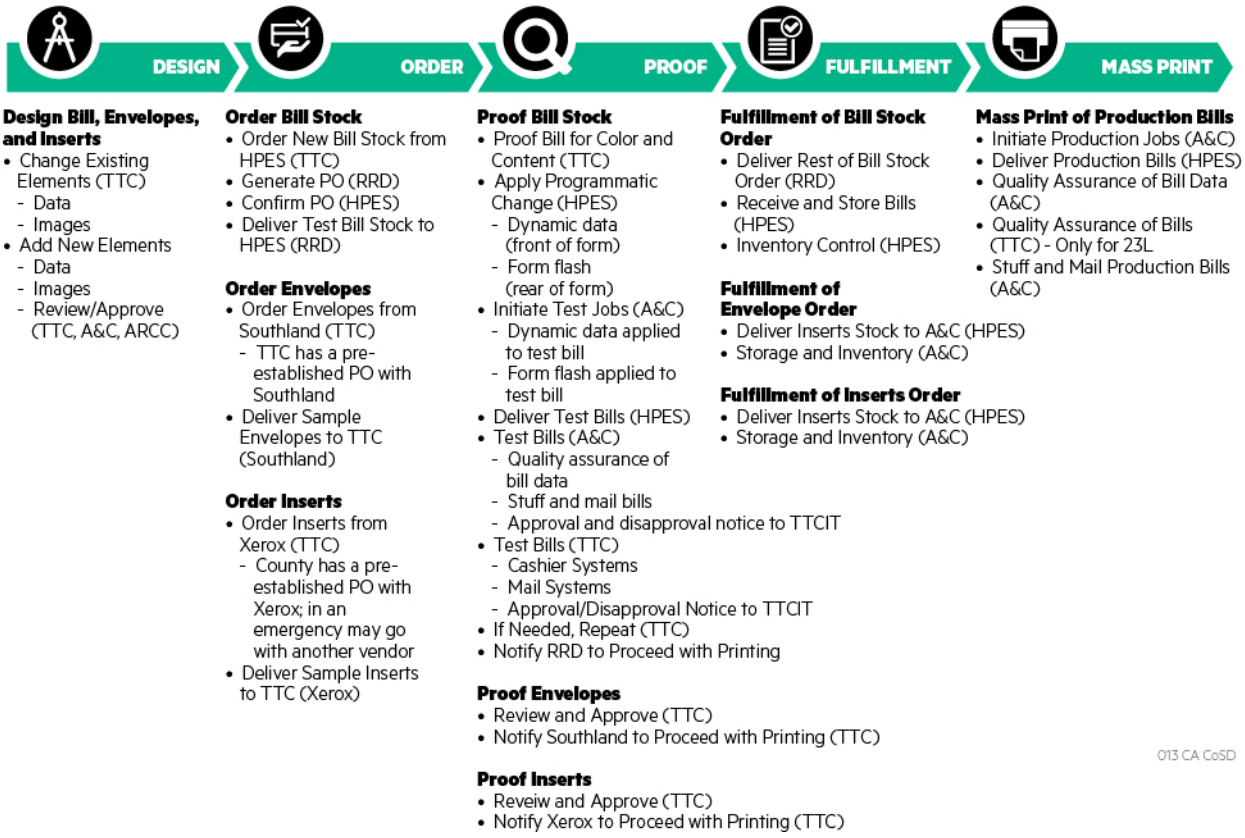
Figure 119. HPES Process for Receiving and Printing Reports



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.

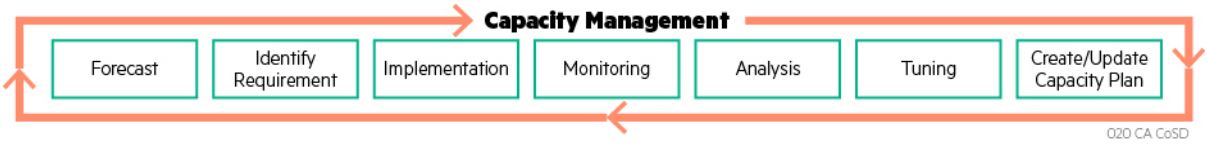
Methodologies to reduce license obligations for server/CPU/core based licenses shall include switching licensing models between host-based and guest-based metrics (when offered by vendor), eliminating redundant licensed passive environments, restricting guest resources, and reduction of capacity dedicated 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.

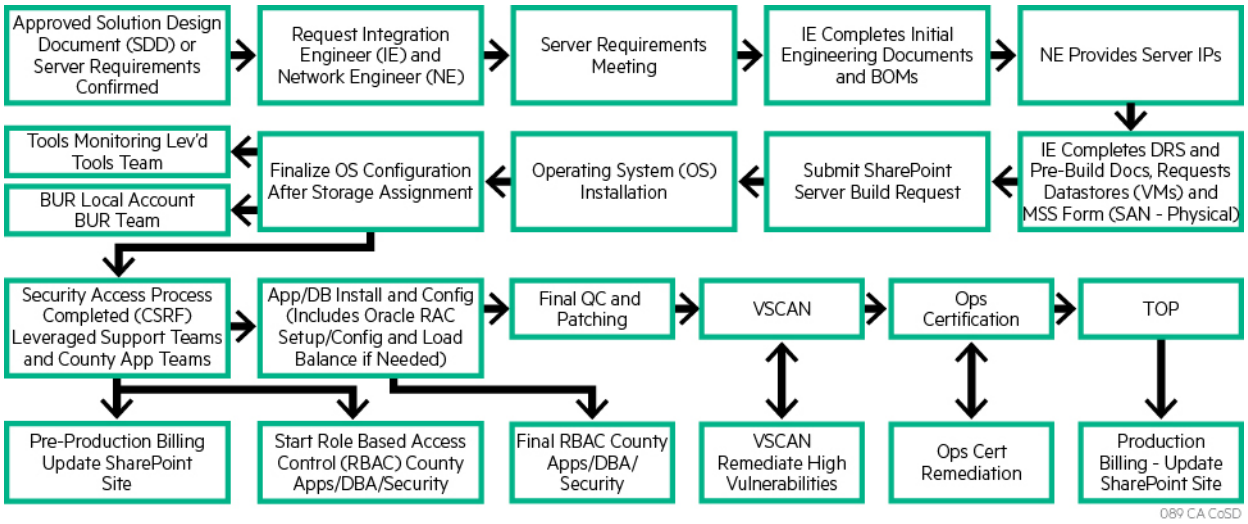
Traditional Provisioning: Using HMCB, we can perform automated provisioning of VMware servers in the traditional environment. Over the long term, we recommend that all VMware environments within the data center be moved into the MPC and the HMCB provisioning process be used for non-data center servers. 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.

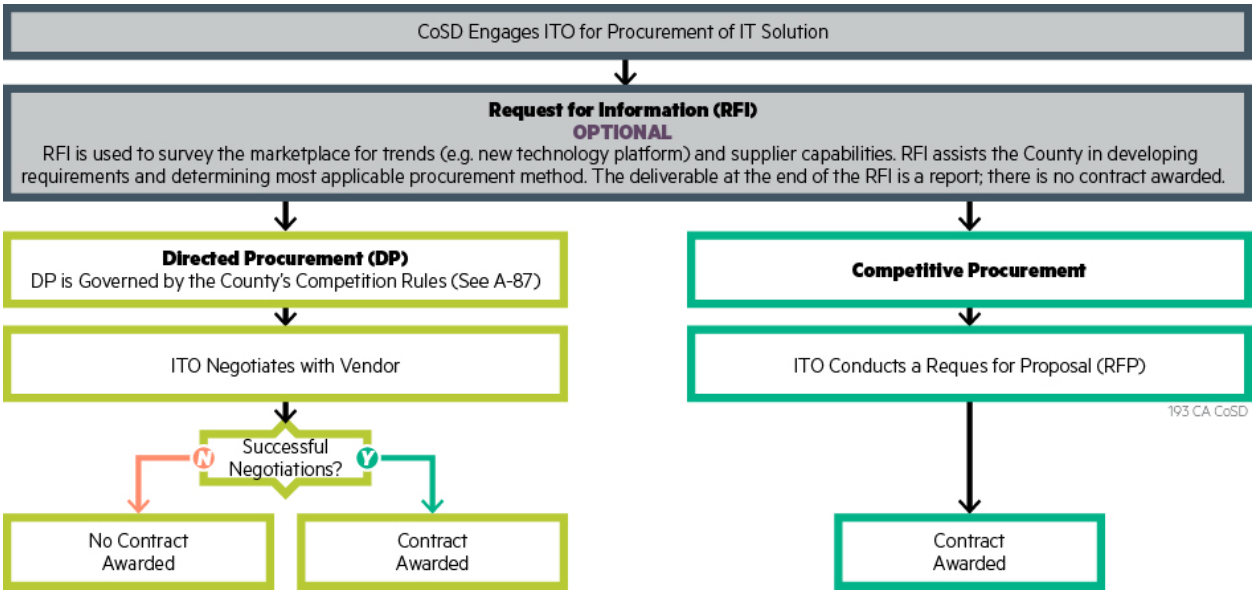
HPES will reach out to application providers who can deliver quality apps projects on time and within County budget. As builder for some, broker for all, we do not assume HPES must develop all County projects with HPES personnel. We will work to include applications providers such as SAIC and CGI in 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.

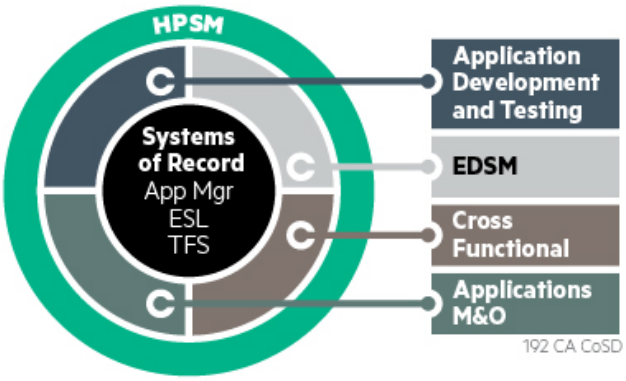
HPES will create, update, and maintain a QA management approach for applications updates. This approach includes the following QA components:

- 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.

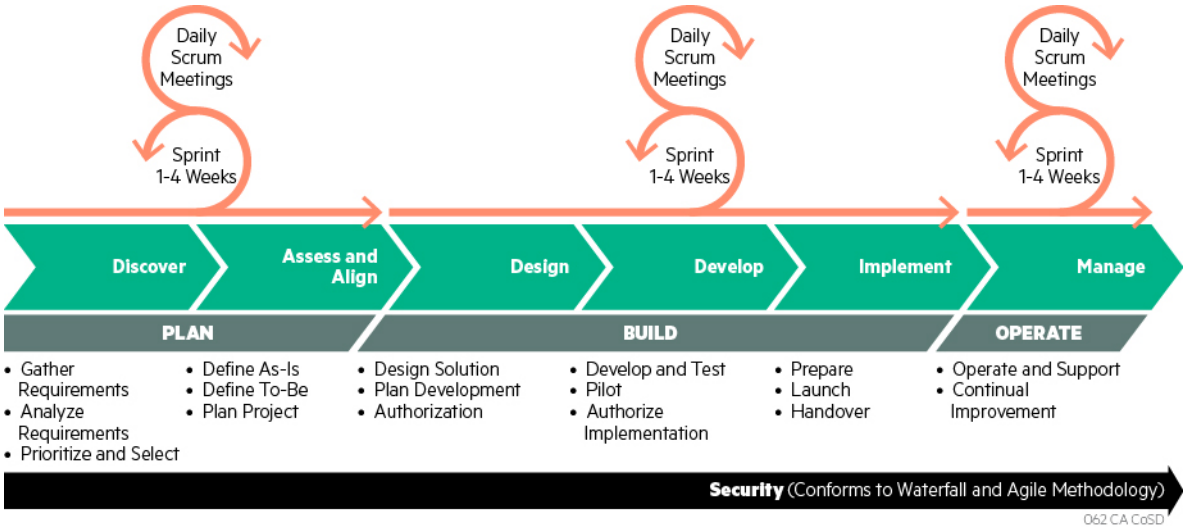
None.

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



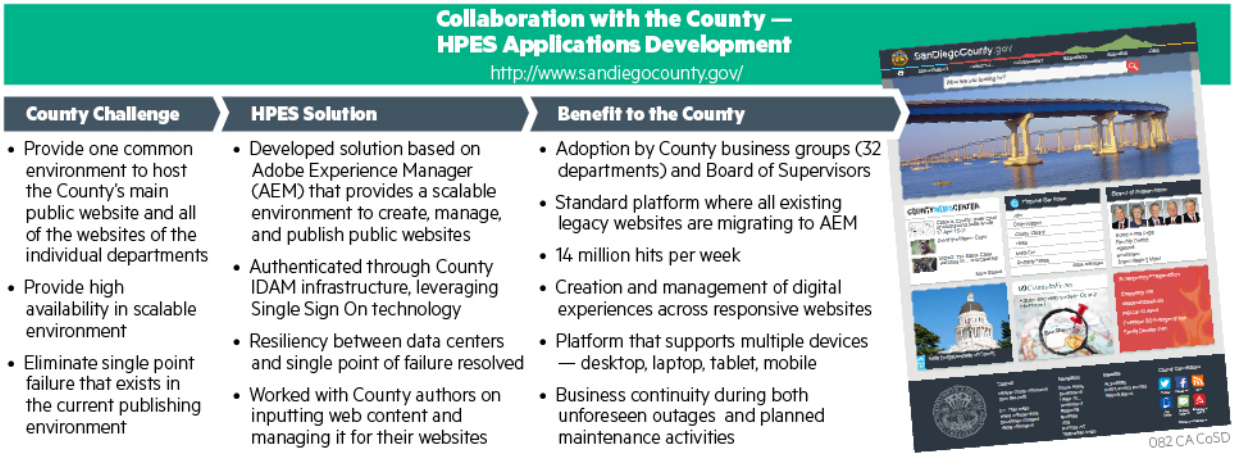
Our framework spans the full delivery life cycle.

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.

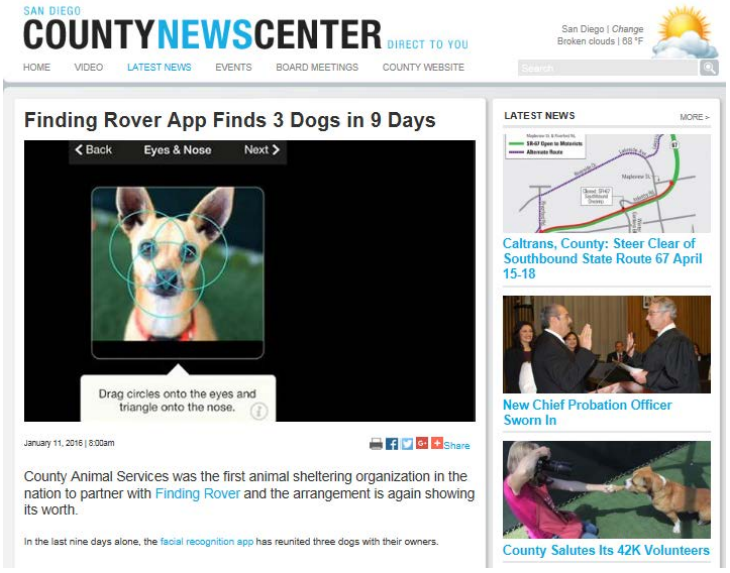
Deliverables for the assets and align phase include:

- 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.

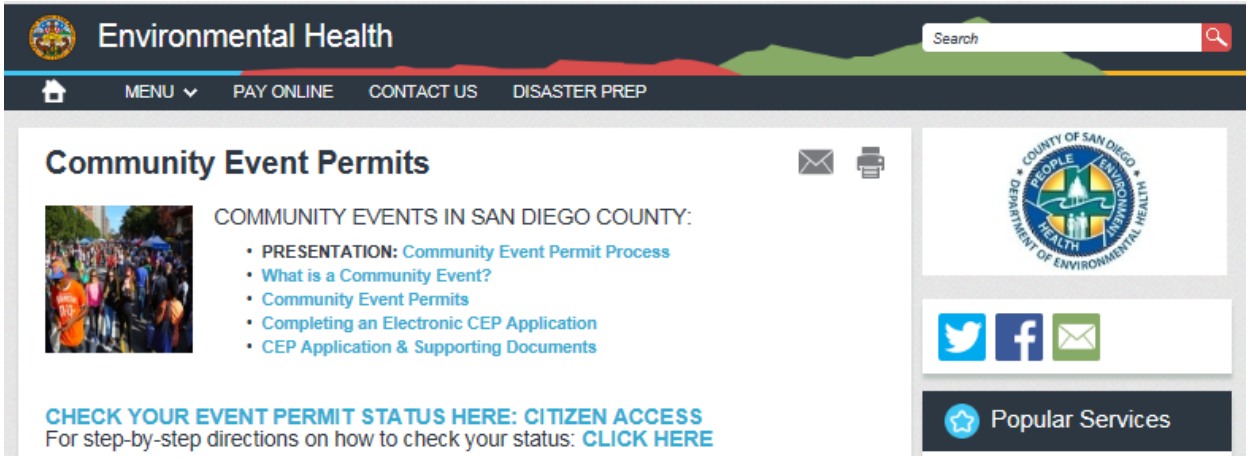
During this phase, application developers will implement the application according to the functional specification and application architecture. The developer will follow Software Development Lifecycle standard County process and standards to code, build, and deploy. The configuration changes will be 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.

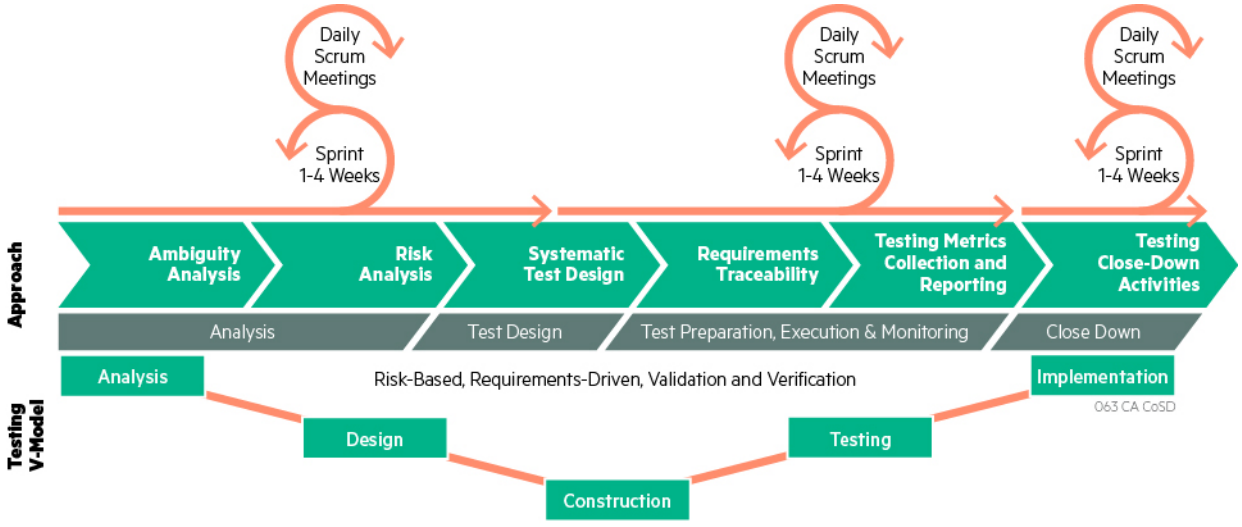
HPES uses a proven set of tools (like HPE's Project and Portfolio Management Center (PPMC)) to plan, budget, and track cost, scope, and schedule performance data. Our use of these tools, combined with our best practices and project management methodology, provides an accurate and responsive automated 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

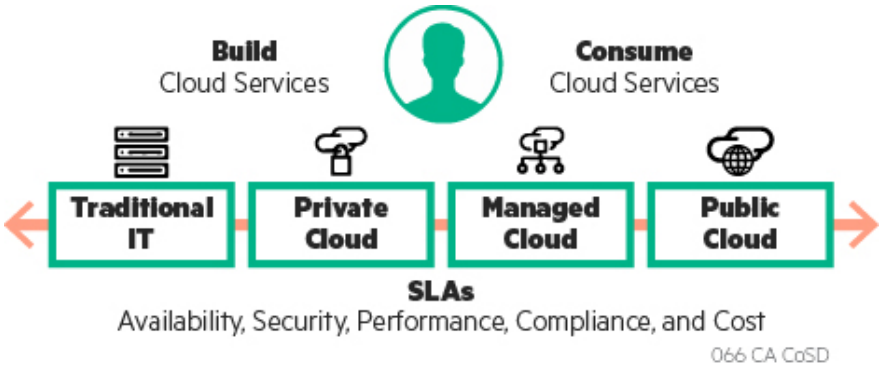
As a global leader in cloud services and technologies, HPES has been delivering compute services in a utility, pay-as-you-go model for more than 10 years—before advent of the term "cloud." With the planned consolidation to the Tulsa data center, HPES will take this opportunity to move the current dev/test 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.

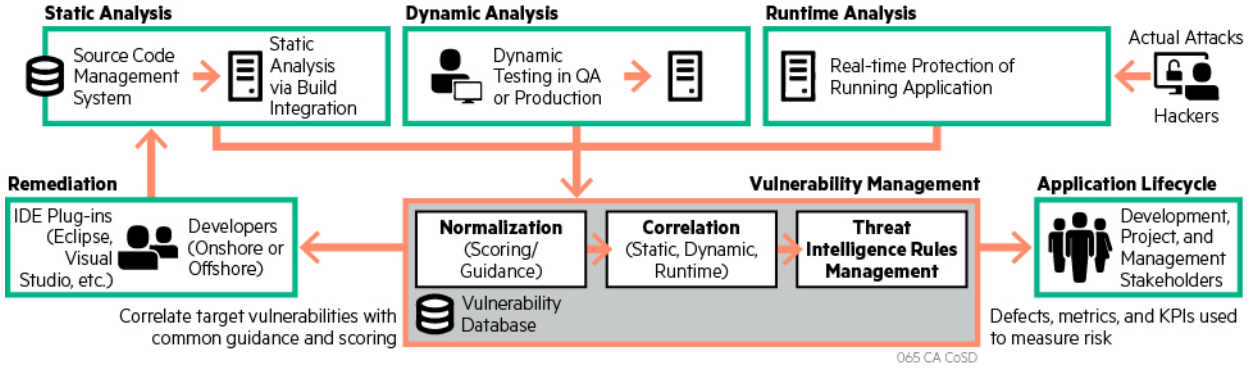
HPES Cloud System enables our development team to build and manage services across private cloud environments on a simplified, integrated architecture:

- 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



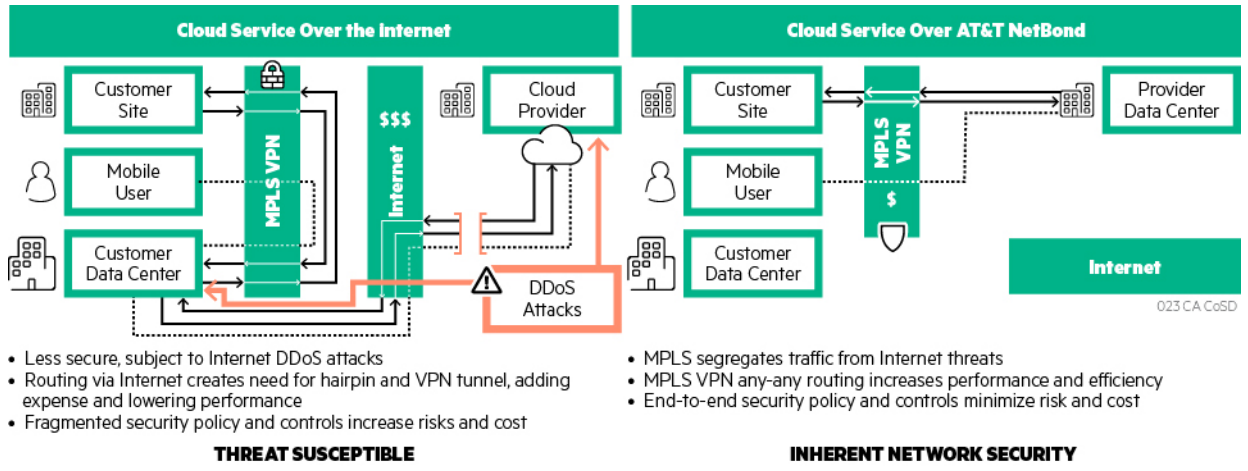
HPES will provide a, short-track implementation into the County environment that will result in a scan of the target application. This will enable our team to accomplish the following:

- 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:

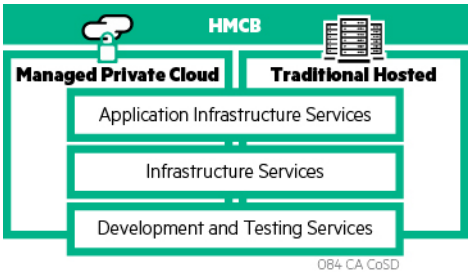
- Leverages a modern, easy-to-use self-service portal with an intuitive shopping cart experience for ordering infrastructure and application services across both private and public cloud environments.
- Enables an open, heterogeneous, and extensible architecture supporting OpenStack-based cloud standards, 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.

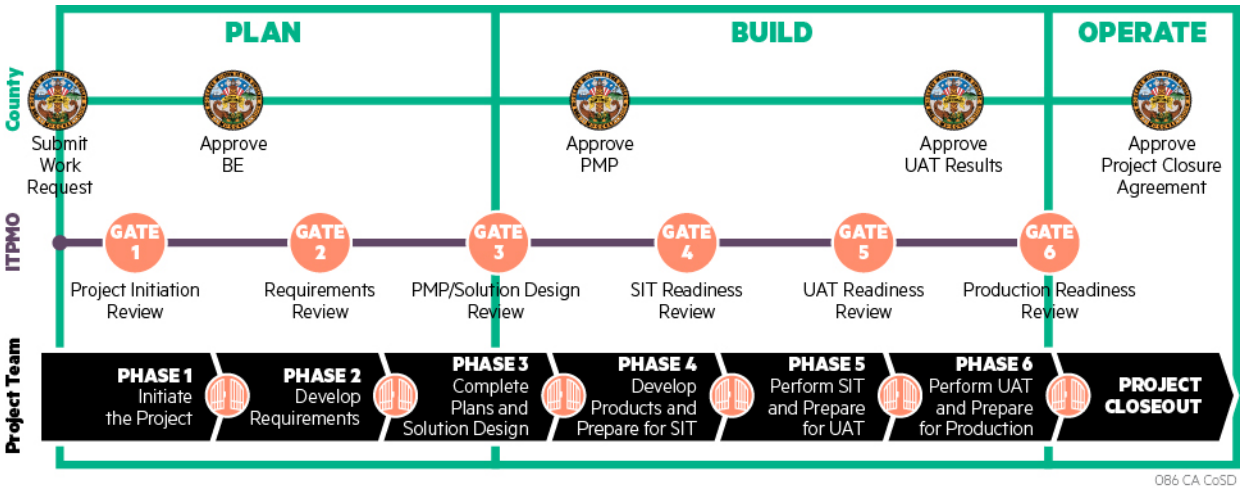
The HPES Waterfall approach used at the County consists of various phases, Waterfall steps and approvals, and checkpoints, as depicted in Figure 138.

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.

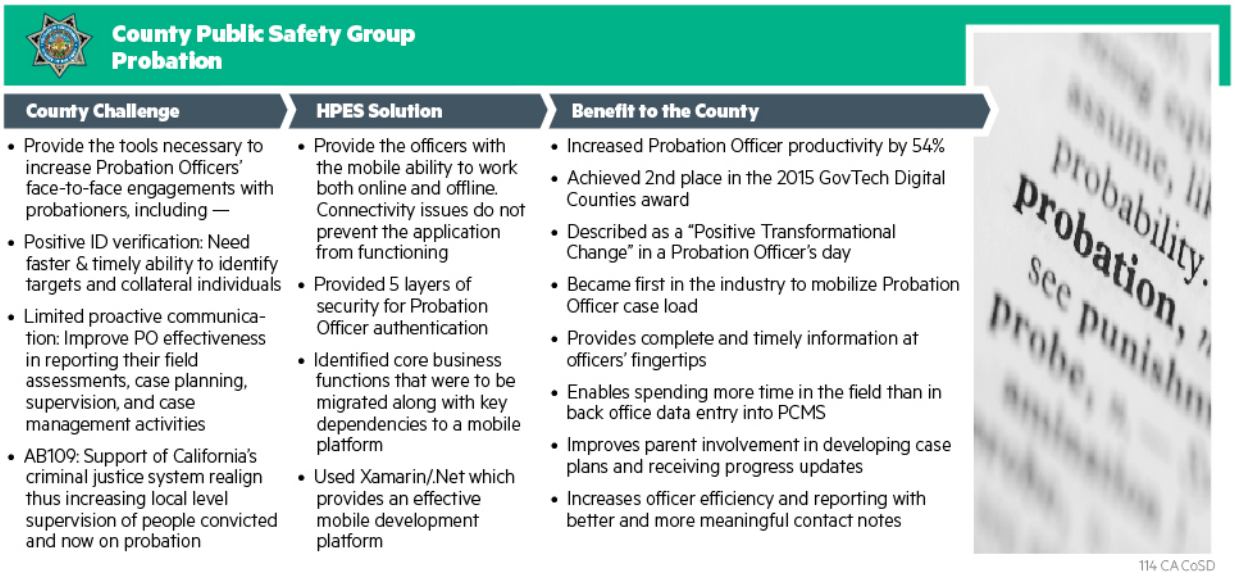
In situations that call for lean software development, HPES tailors an Agile development approach for each project. Based on the Scrum framework, this approach uses an appropriate selection of sound engineering practices from Extreme Programming (XP). It provides a substantial benefit by enabling rapid 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.

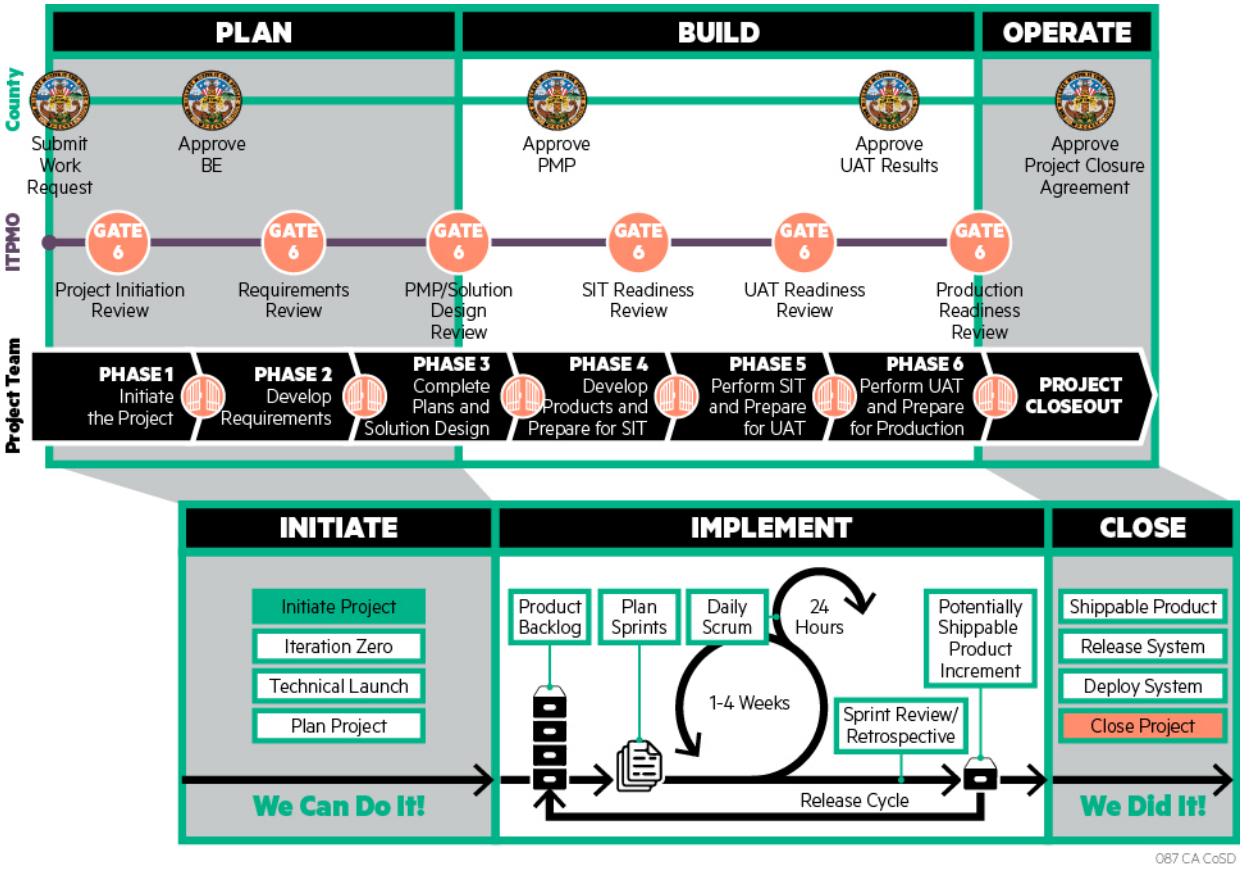
The sprint length is usually consistent over the course of the project, and sprints follow one after the other without pause.

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.

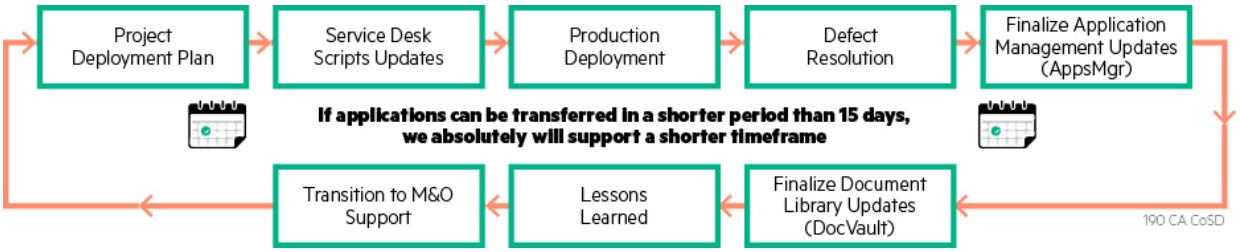
When adding an application to the M&O portfolio, unless modified by a Service Request, Portfolio Applications shall be added into the appropriate FFP M&O bundle immediately upon implementation into production or the expiration of a stated warranty period, whichever is later. Addition includes updated 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:

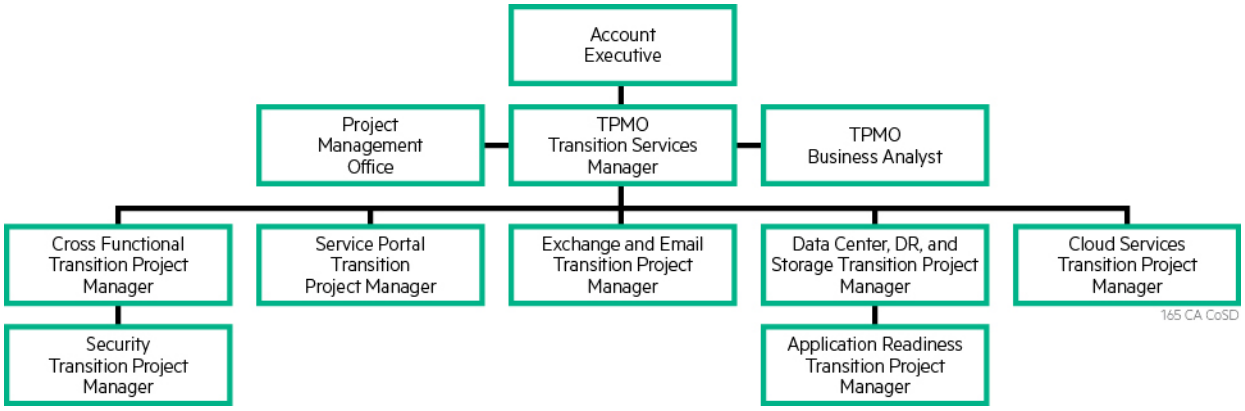
FRAMEWORK	TRANSITION PLAN
Service Desk	• Cross Functional Transition Schedule and Tasks, Page 506 • Response to Section 3.6, Page 511
Application Services	• Cross Functional Transition Schedule and Tasks, Page 506 • Special Cross Functional Projects – Application Services Framework, page 511
End User 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.

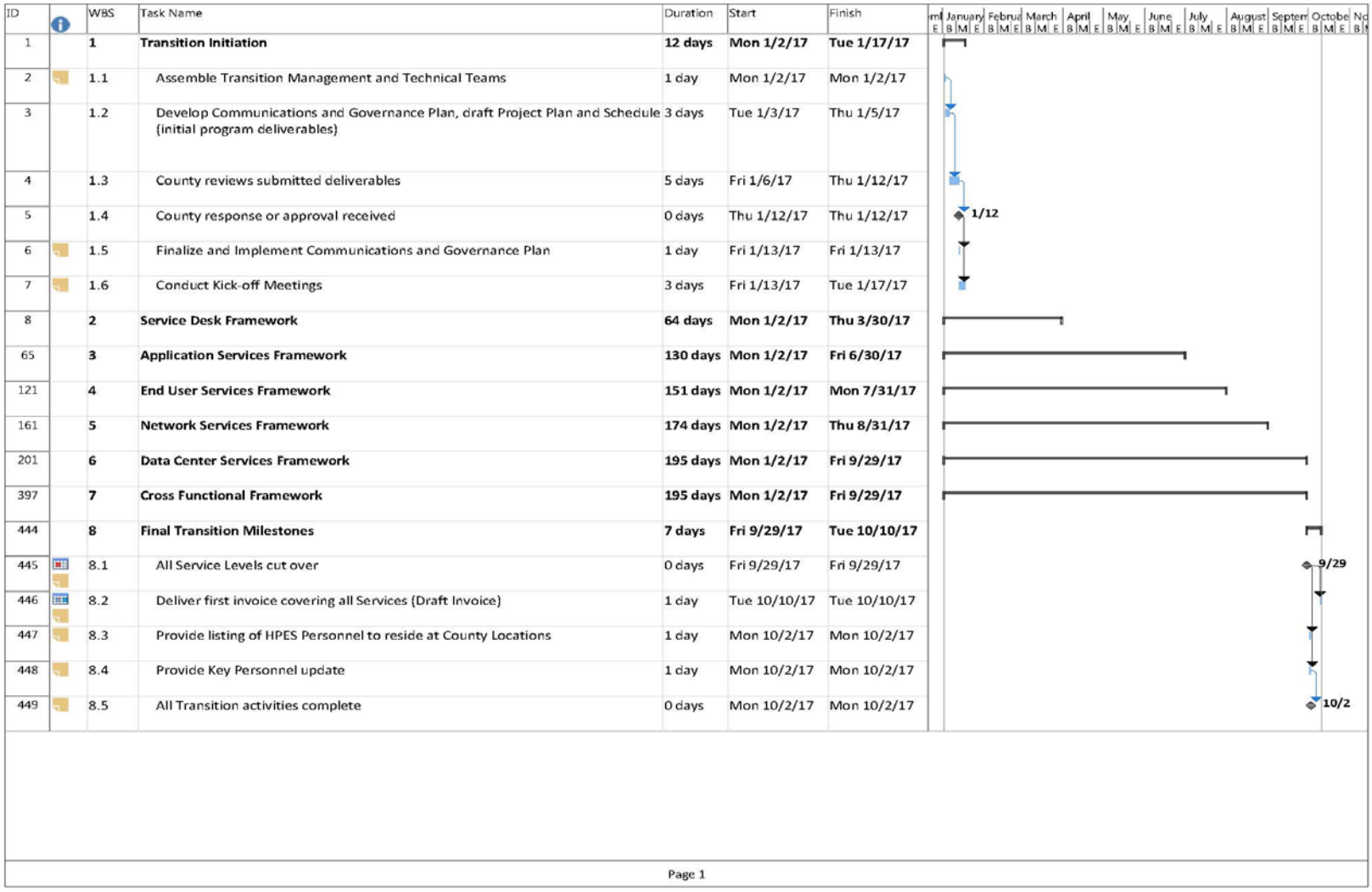
Transition programs and their associated projects will go through five distinct phases: Initiate, Plan, Execute, Monitor and Control, and Close.

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.

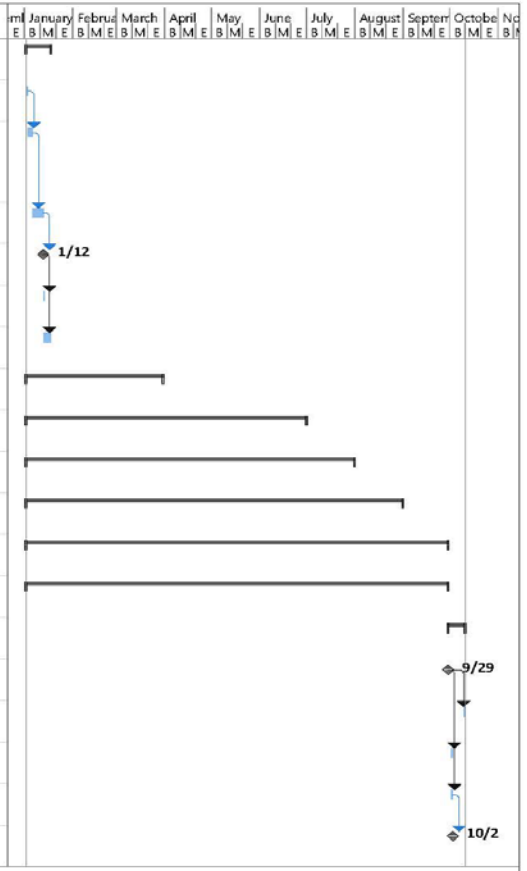
There are no dependencies identified for generation of the Cross Functional Component Management Plans. They will be developed in parallel with, and as the culmination of, the other component artifacts.

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.

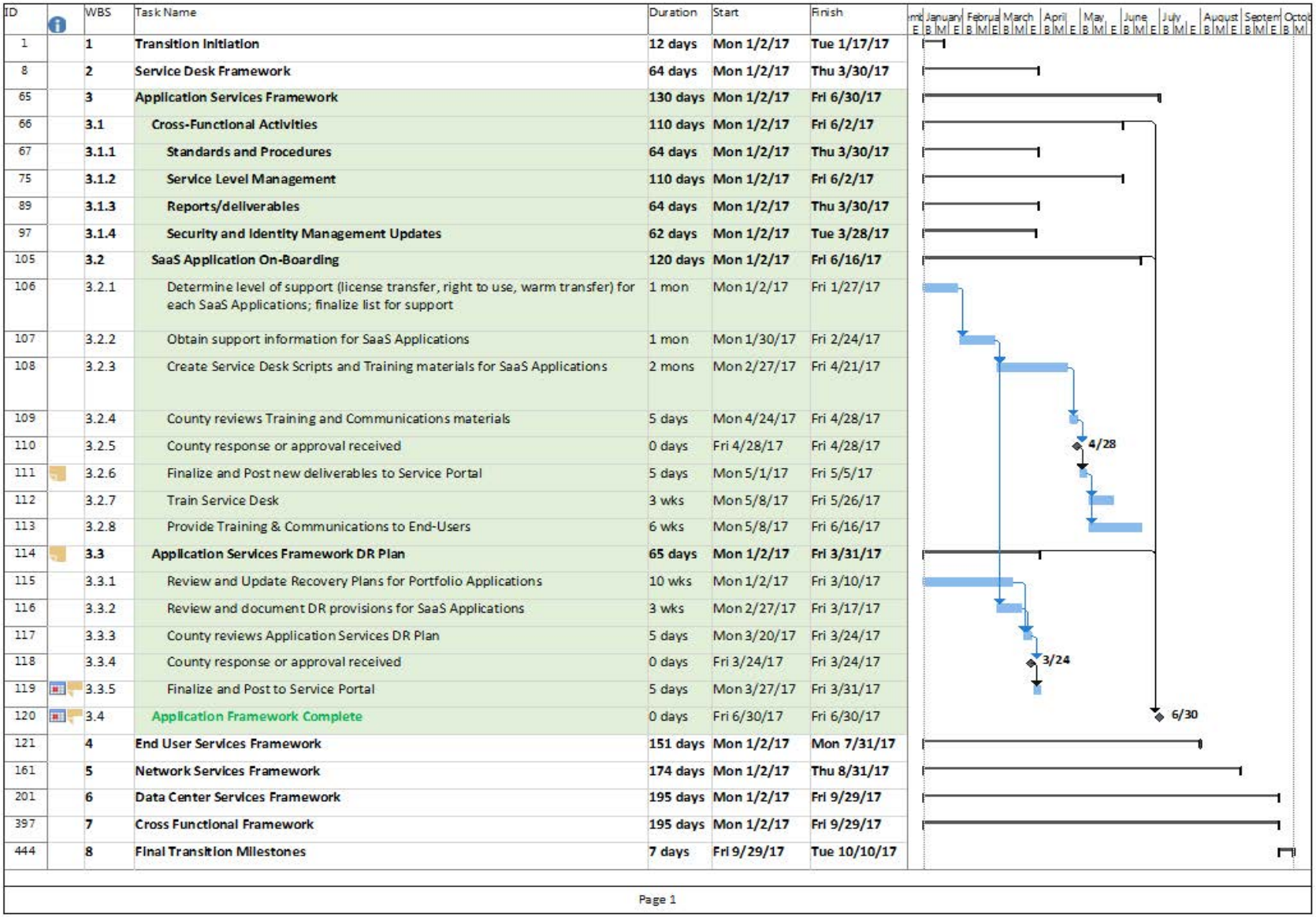
We will review each application that the County wants us to support, according to our established process for Third Party Agreements, and determine the level of support possible for each (license transfer, right to use, warm transfer). Once we have a final list, we will work with the support contacts 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

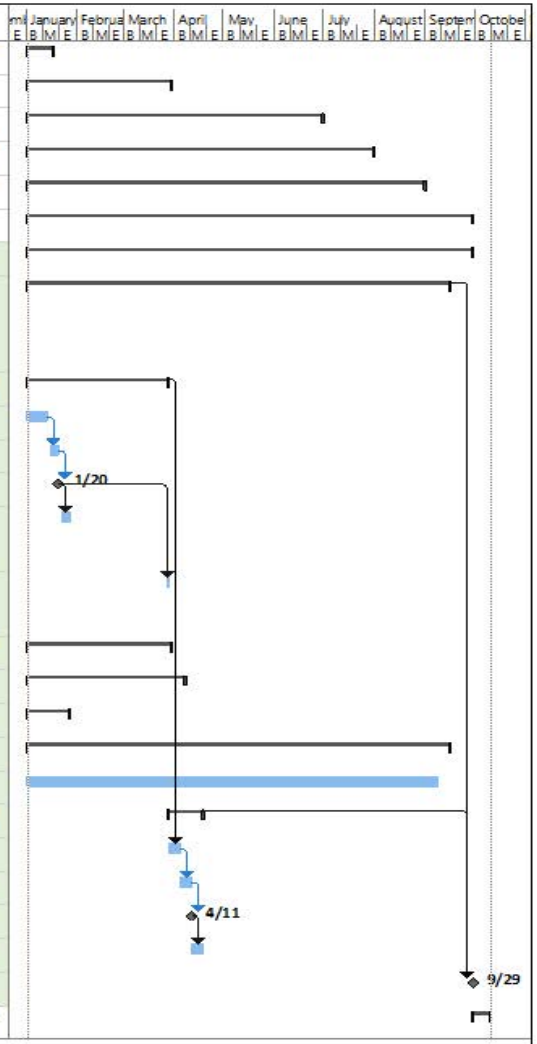
FRAMEWORK COMPONENT	EXTENT OF CHANGE	SPECIAL PROJECTS OR CONSIDERATIONS
Contract and Acquisition Management Services	Minimal	None
Integrated Asset Management Services	Limited	We will integrate data from AT&T Asset Management Systems
Billing Management Services	Limited	Setup of billing processes for new 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).

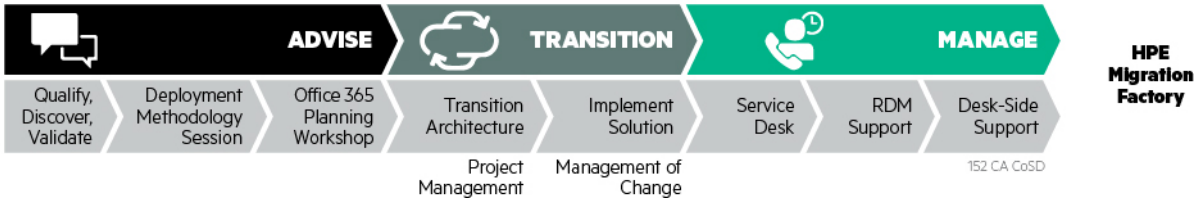
- Methodology & Key Processes – Key methodologies and processes in proposed solution

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

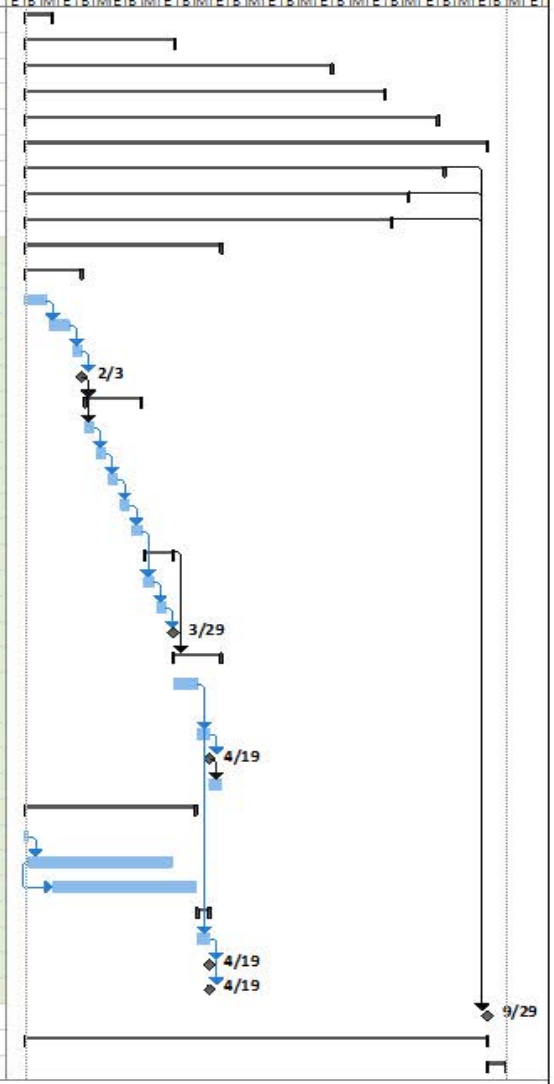


Transition Schedule and Tasks

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

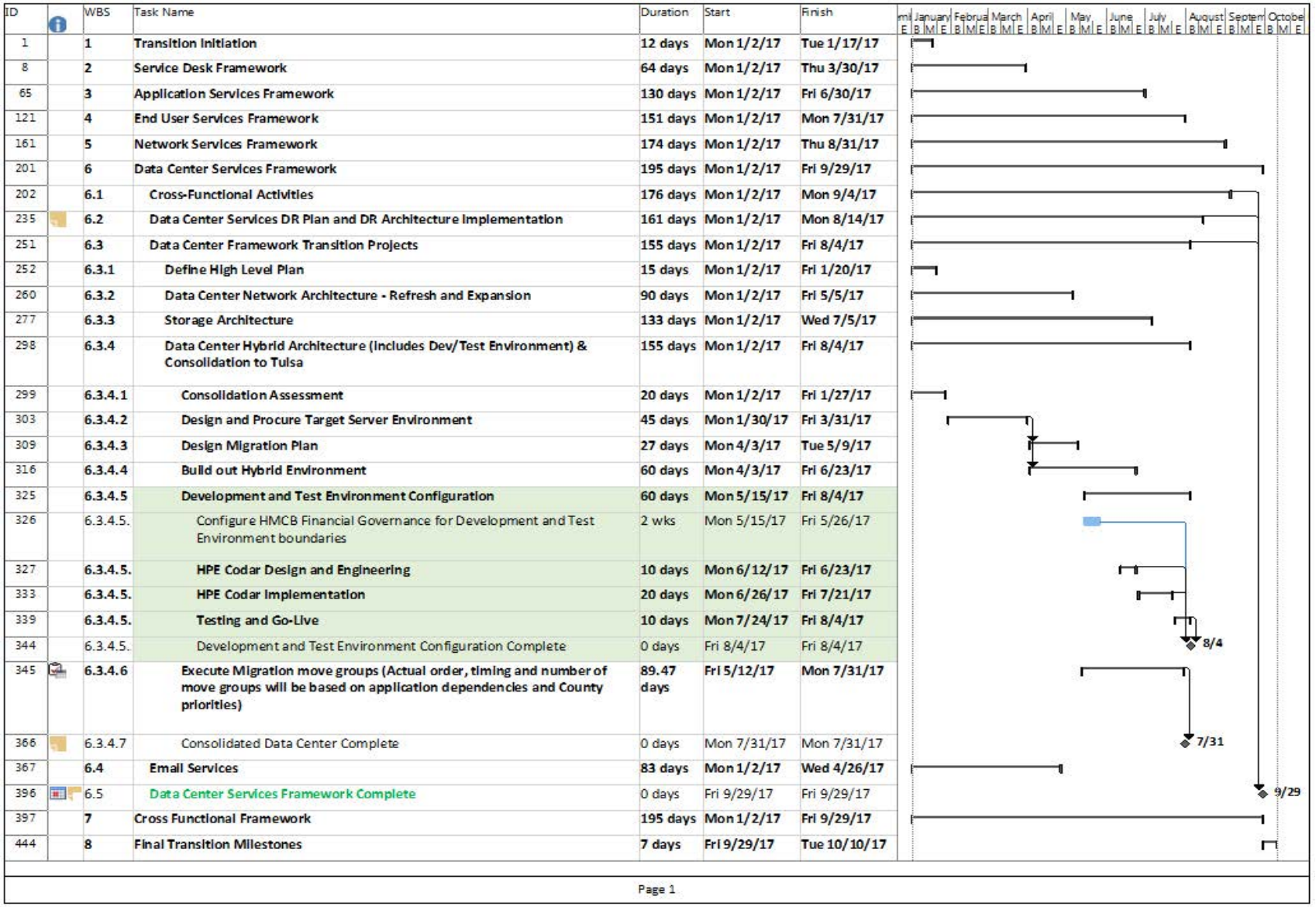
The Data Center Consolidation Transition Plan, shown in Figure 149, includes the activities required for the Dev/Test environment transition to the hybrid cloud; these are described as part of the Data Center Consolidation Transition Project. Those tasks unique to the Dev/Test environment begin where 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.

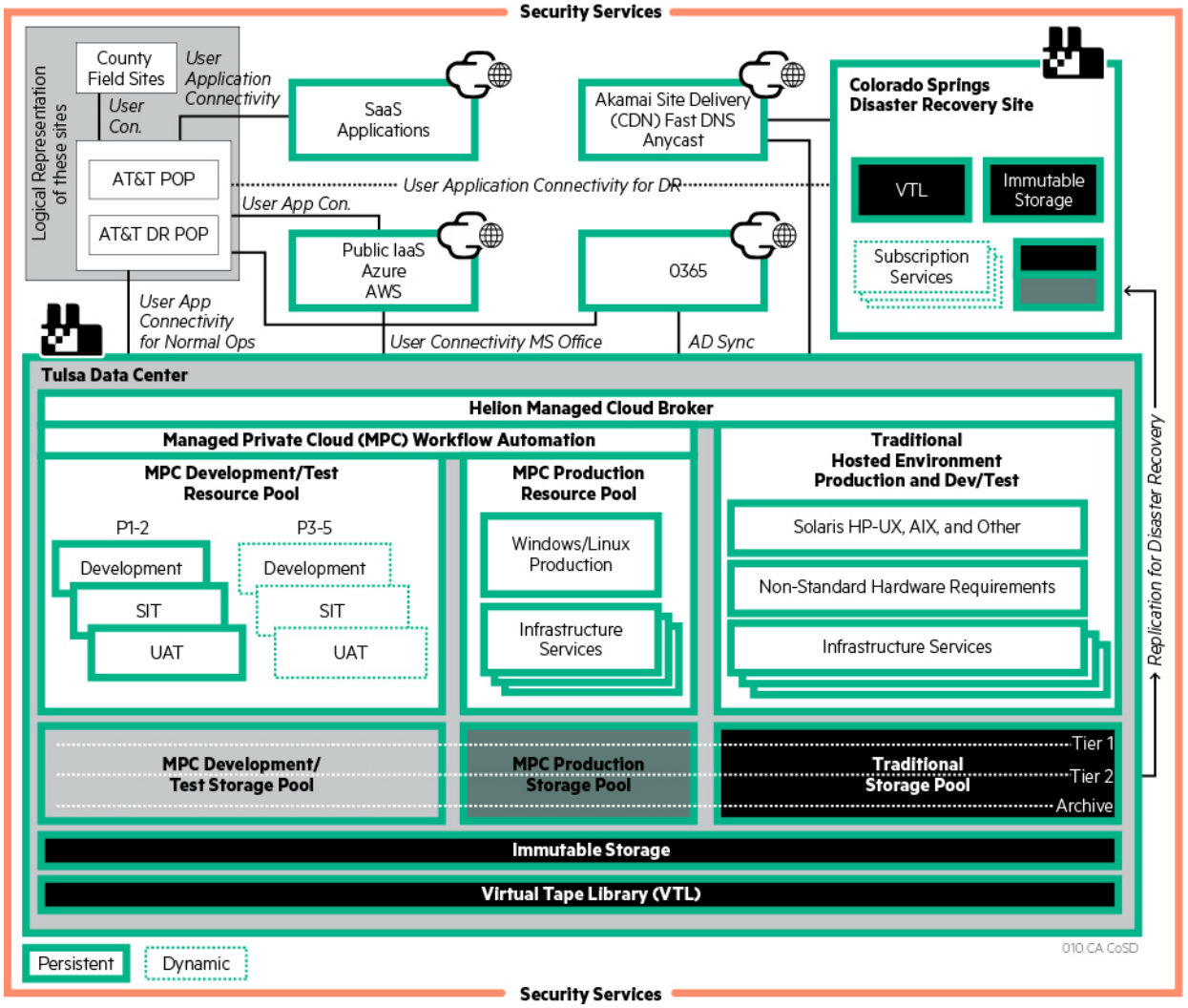
Our structured transition approach for the data center consolidation is comprised of the following subprojects. These will be completed in the sequence listed below to accomplish a smooth and nondisruptive transition.

- 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

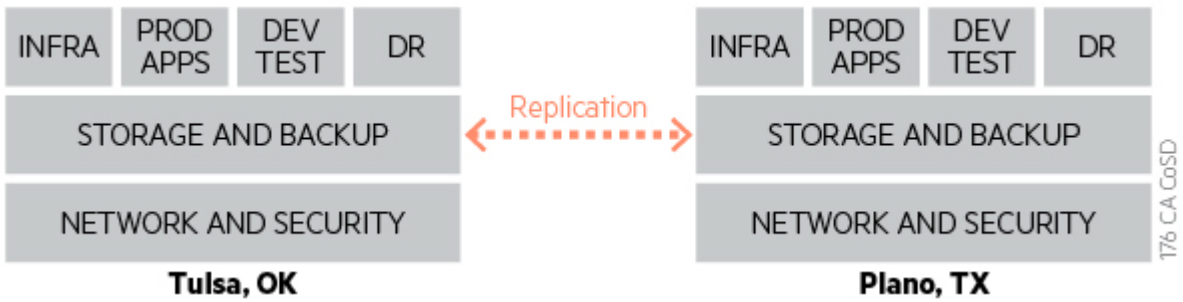


The Data Center Consolidation will result in a modern hybrid environment.

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.

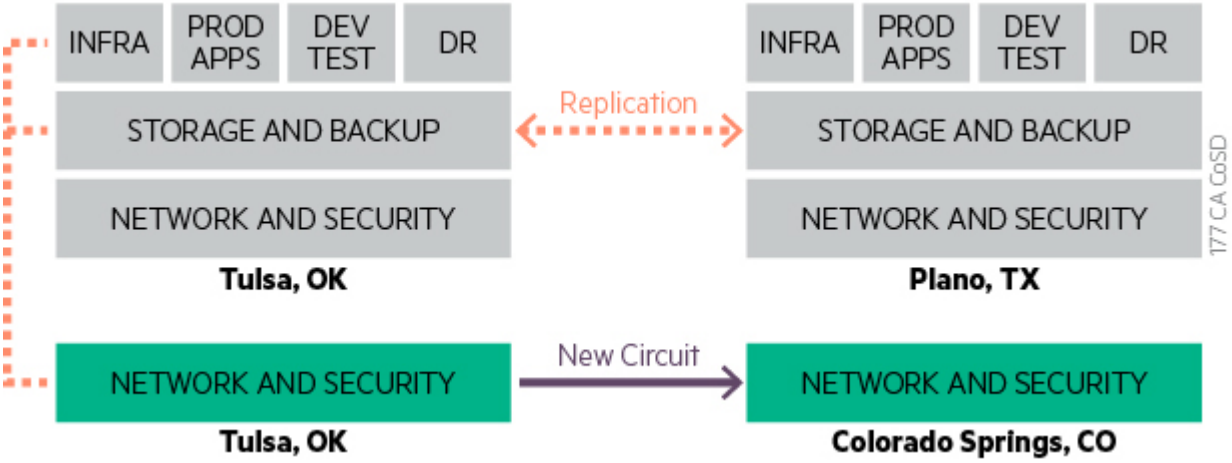
Figure 151. Current Data Center Environment



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.

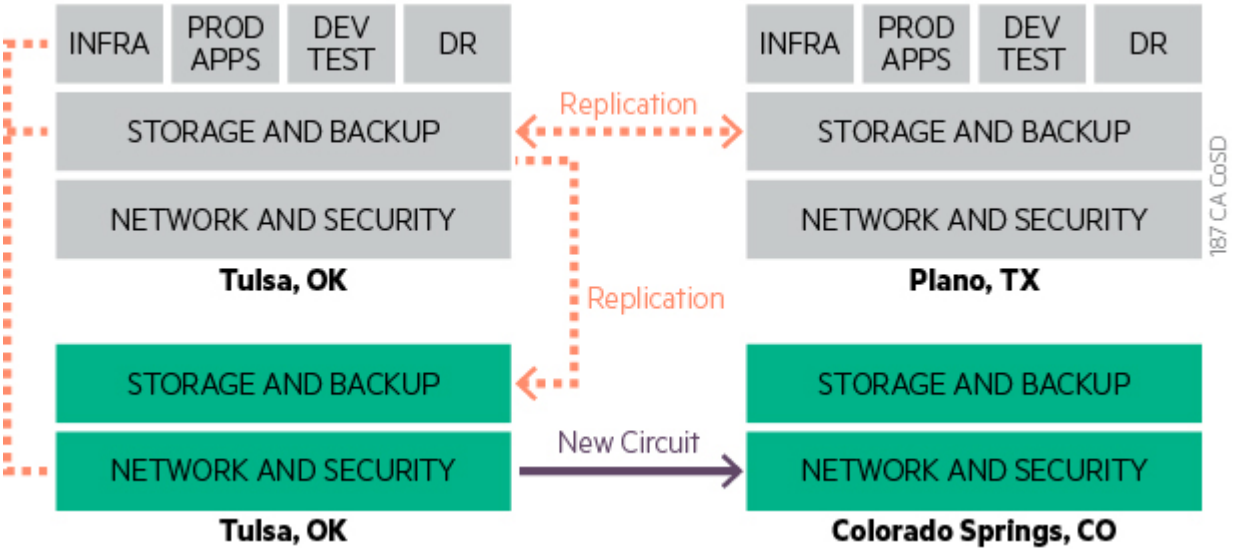
Storage Architecture.

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.

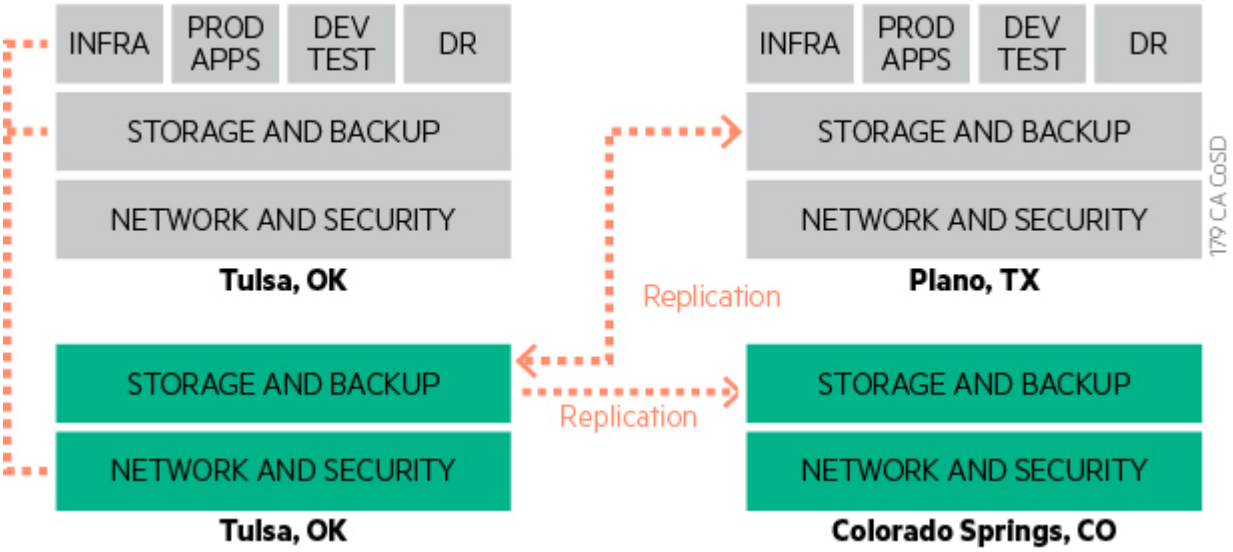
Figure 153. Deploying New Storage, Migrating Data



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

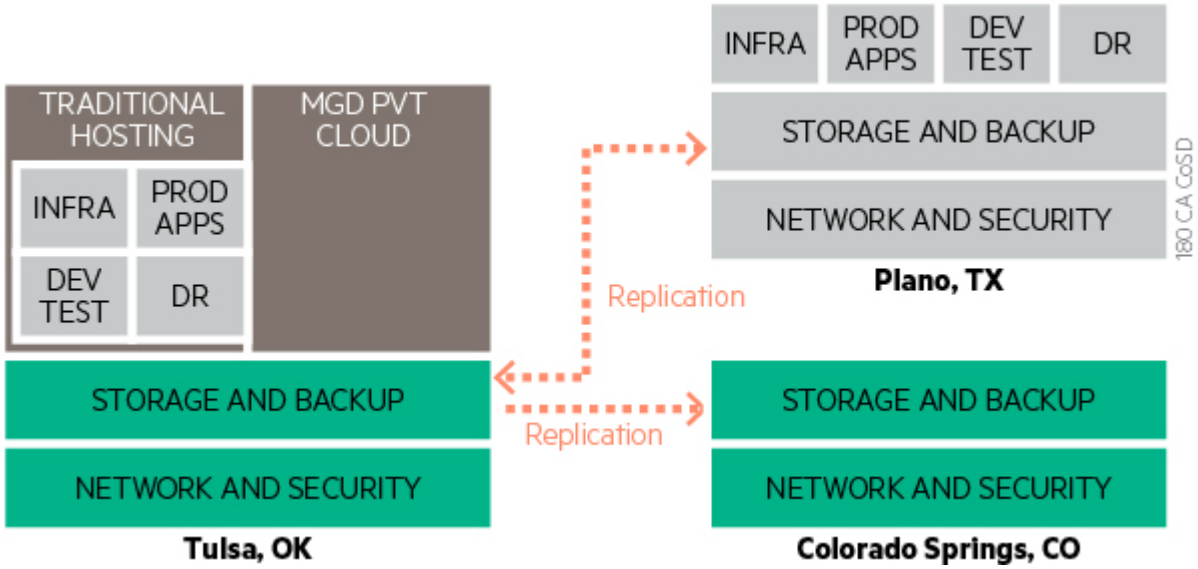
In order to avoid migrating End-Users' Home drive storage twice, the County may wish to migrate this data to OneDrive for Business (ODfB) as defined in the User Data Services Transformation Project prior to the storage migration. HPES shall accommodate this request, provided that the County can commit 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



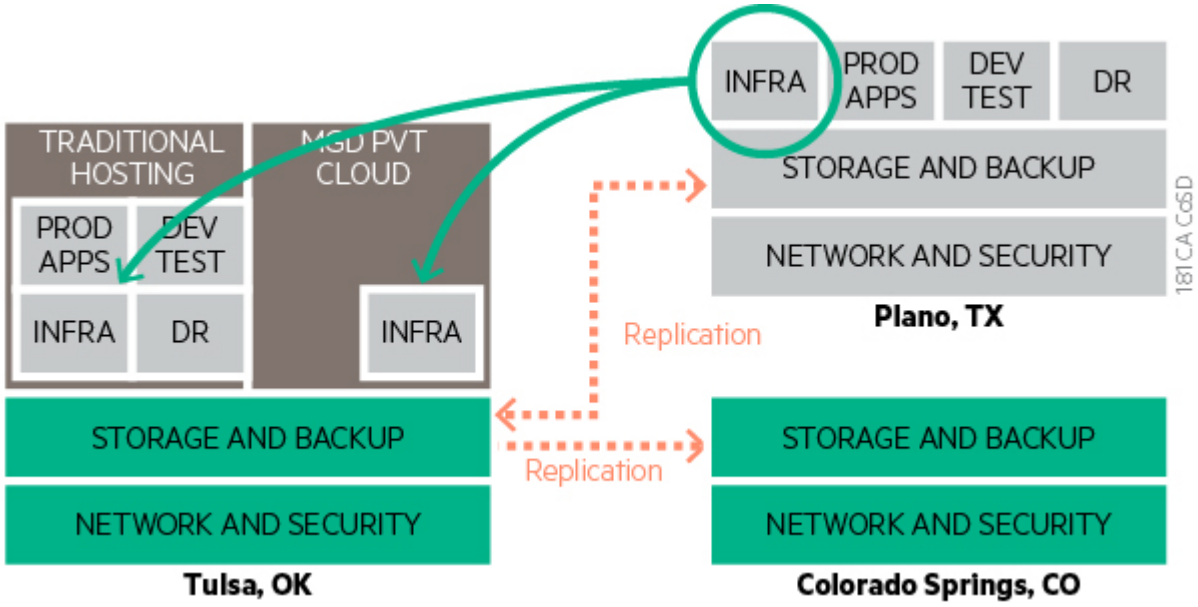
Then we can decommission the old storage and network environments Figure 155. At this point, no migrations have taken place: we have built out the new capacity to support the migration and the hybrid cloud architecture.

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.

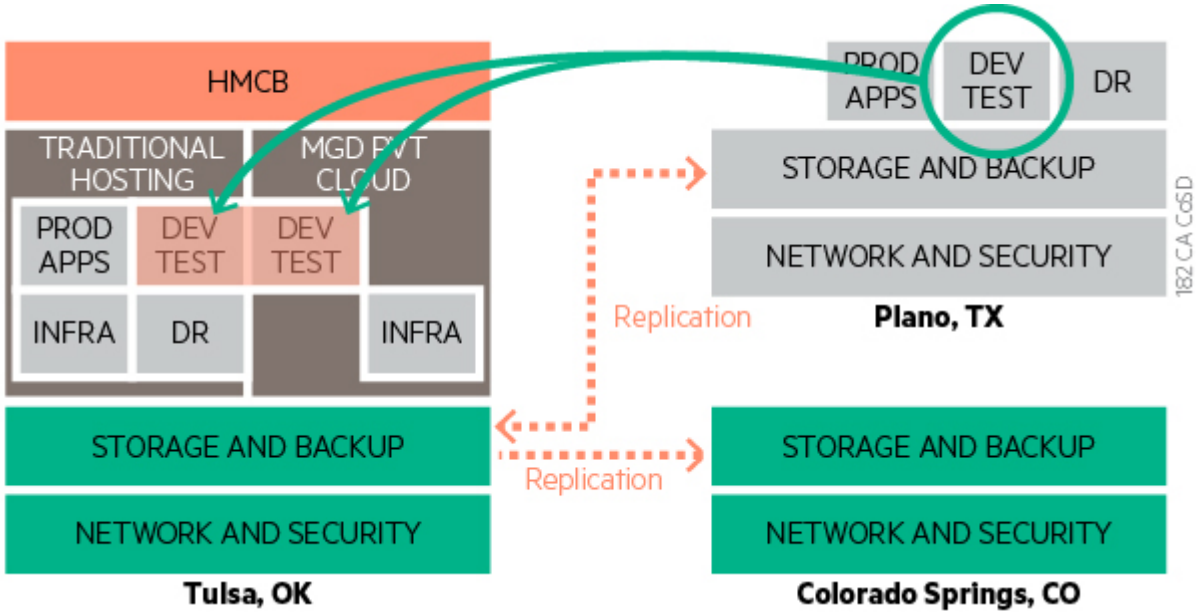
Application servers eligible to be hosted in the MPC include virtual servers that fall into a specific range of sizes, described in detail in Section 2.9,and will run current County approved versions of Windows and Linux.

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.

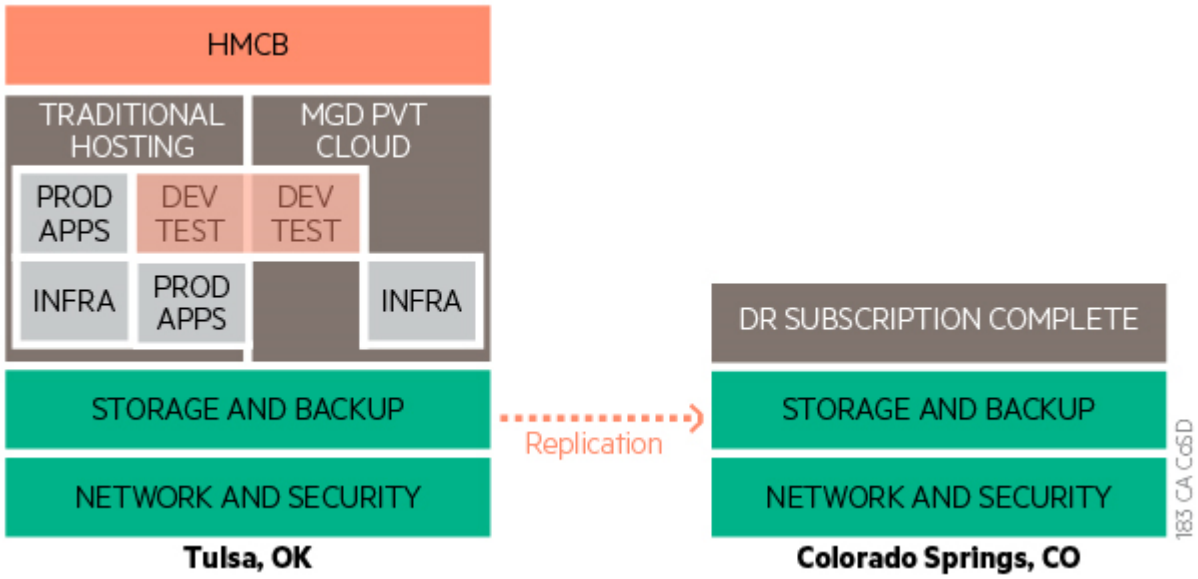
Figure 157. HMCB Deployment, Establishment and Migration into Resource Pools



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.

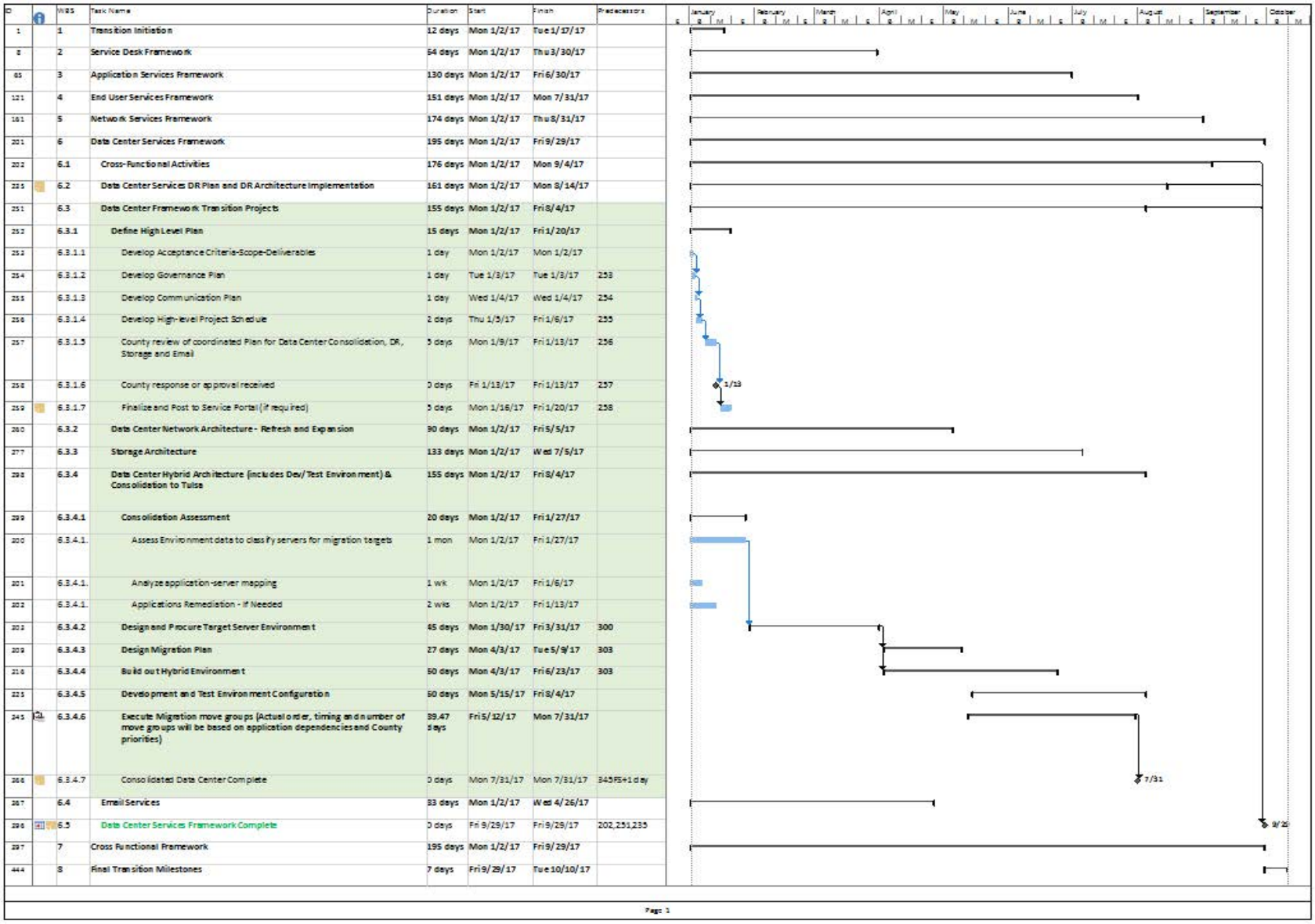
As the network design and buildout is taking place, we will also be analyzing the DR requirements. The draft DR transition plan activities are shown in Figure 161.

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.

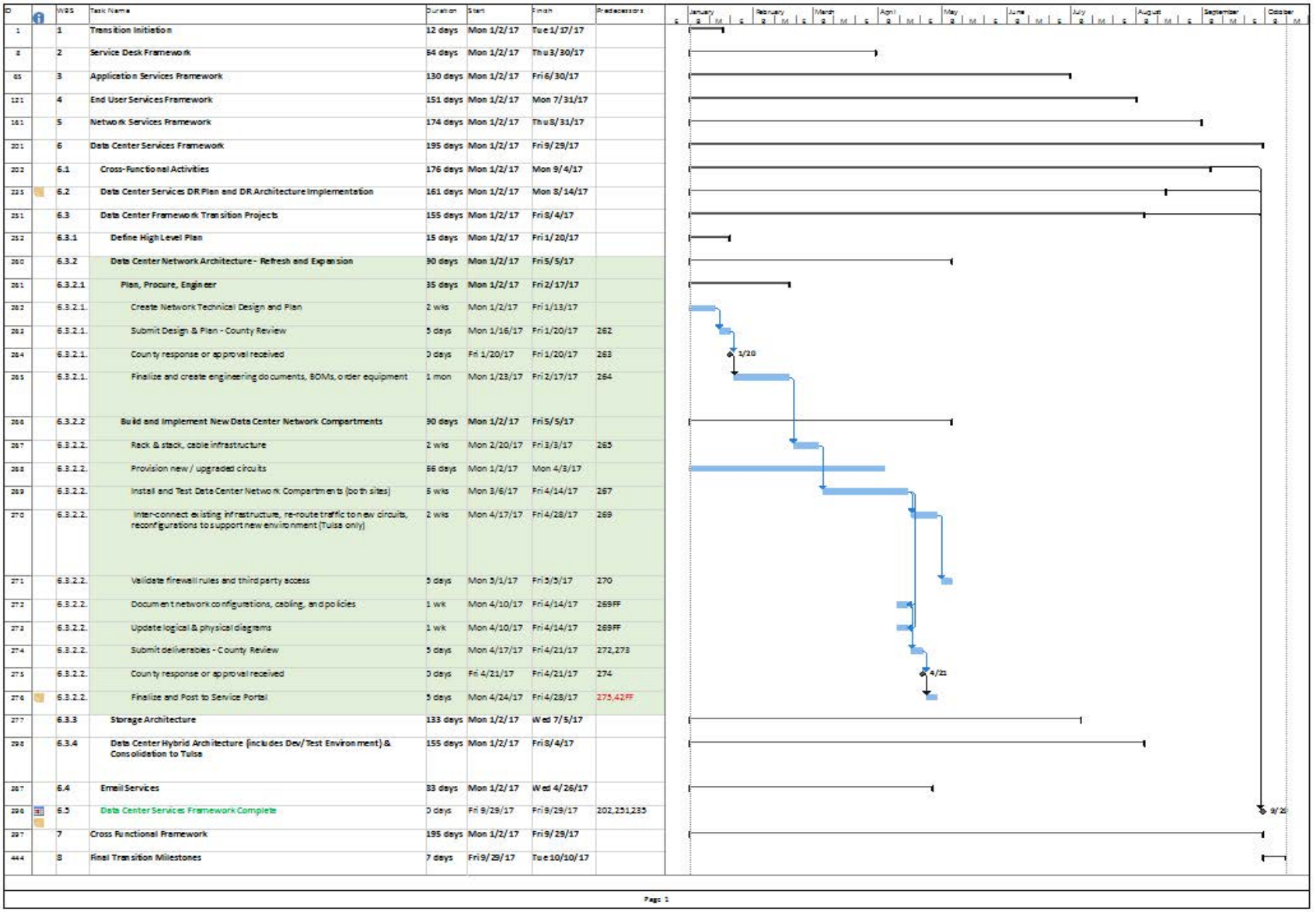
MPC policy and architecture permits creating clusters similar to the production environment to mitigate potential license cost increases.

Figure 159. Data Center Consolidation Planning and Assessment



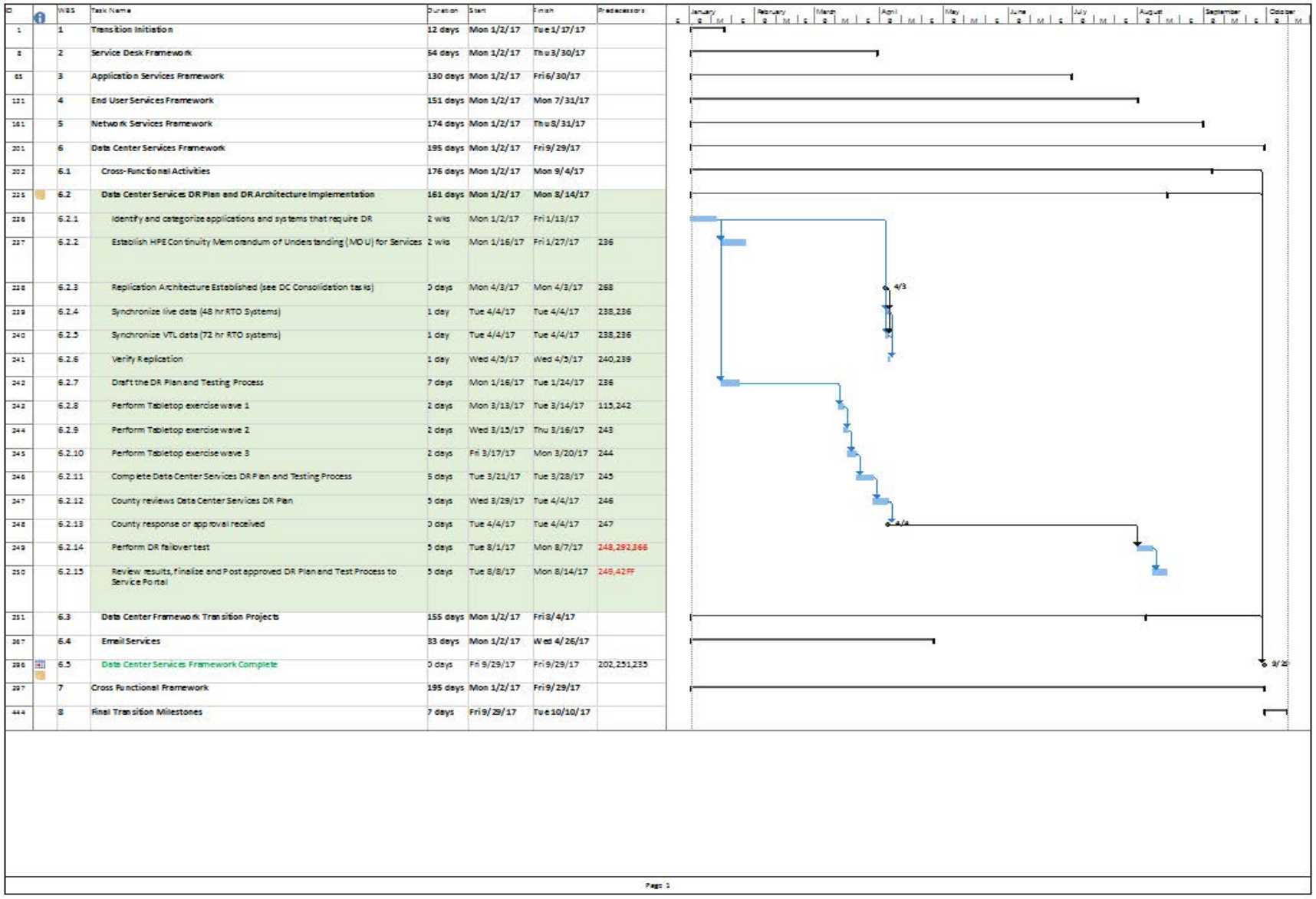
ID	WBS	Task Name	Duration	Start	Finish	Predecessors
1	1	Transition Initiation	12 days	Mon 1/2/17	Tue 1/17/17	
8	2	Service Desk Framework	64 days	Mon 1/2/17	Thu 3/30/17	
65	3	Application Services Framework	130 days	Mon 1/2/17	Fri 6/30/17	
121	4	End User Services Framework	151 days	Mon 1/2/17	Mon 7/31/17	
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	
300	6.3.4.1.	Assess Environment data to classify servers for migration targets	1 mon	Mon 1/2/17	Fri 1/27/17	
301	6.3.4.1.	Analyze application-server mapping	1 wk	Mon 1/2/17	Fri 1/6/17	
302	6.3.4.1.	Applications Remediation - if Needed	2 wks	Mon 1/2/17	Fri 1/13/17	
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
310	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	
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	

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	
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	
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 infrastucture	2 wks	Mon 2/20/17	Fri 3/3/17	265
268	6.3.2.2.	Provision new / upgraded circuits	86 days	Mon 1/2/17	Mon 4/3/17	
269	6.3.2.2.	Install and Test Data Center Network Compartments (both sites)	6 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	
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	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	

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	
131	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	236
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	248,292,366
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	249,42FF
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

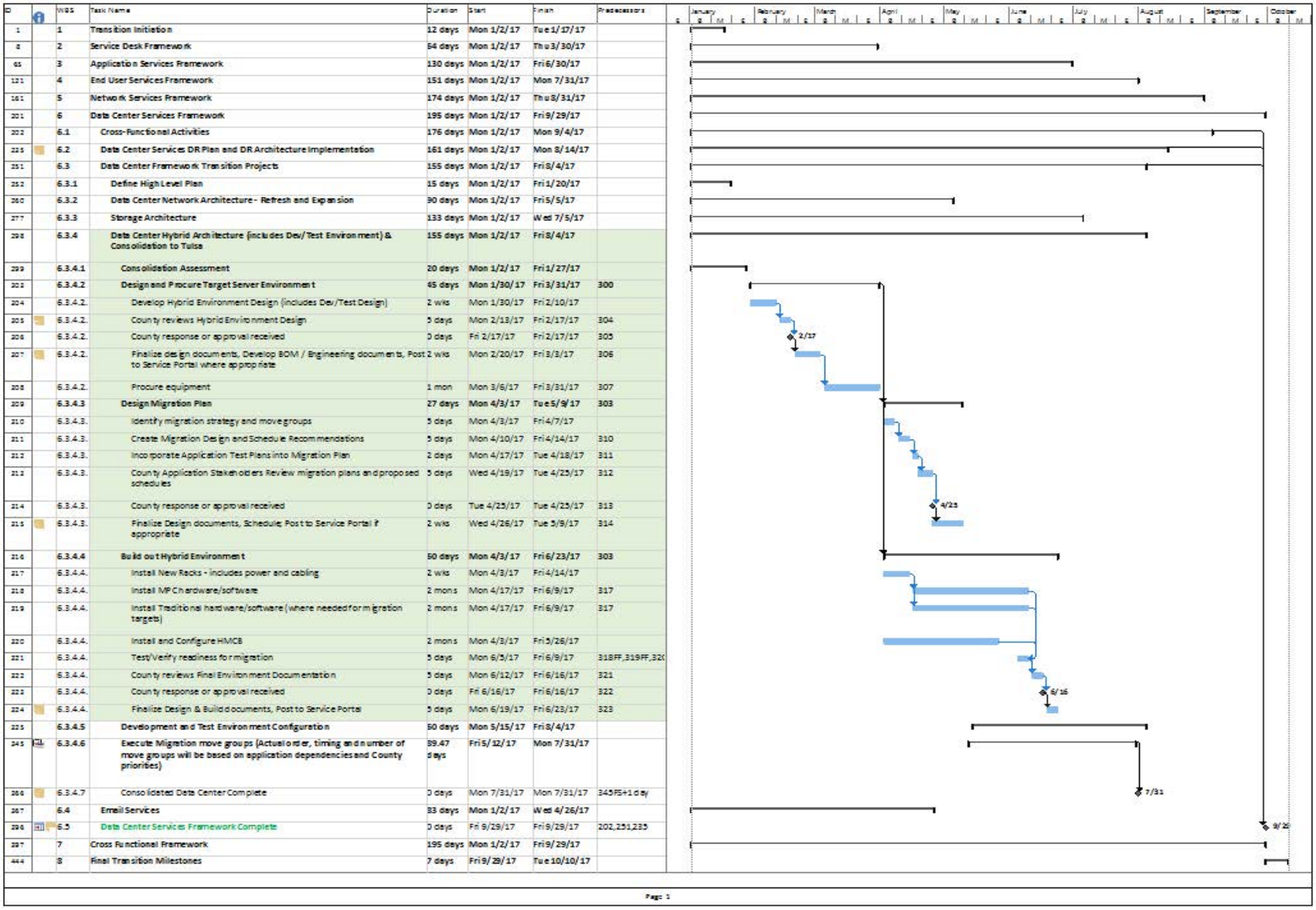
Consolidation Assessment. As described above, we will assess the Plano application and infrastructure environment to identify the migration approach for each. We will prepare a source-to-target mapping that documents each of the servers that will be migrated along with the target server characteristics 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	50 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 MP 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 HMCB	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,320
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	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	
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	

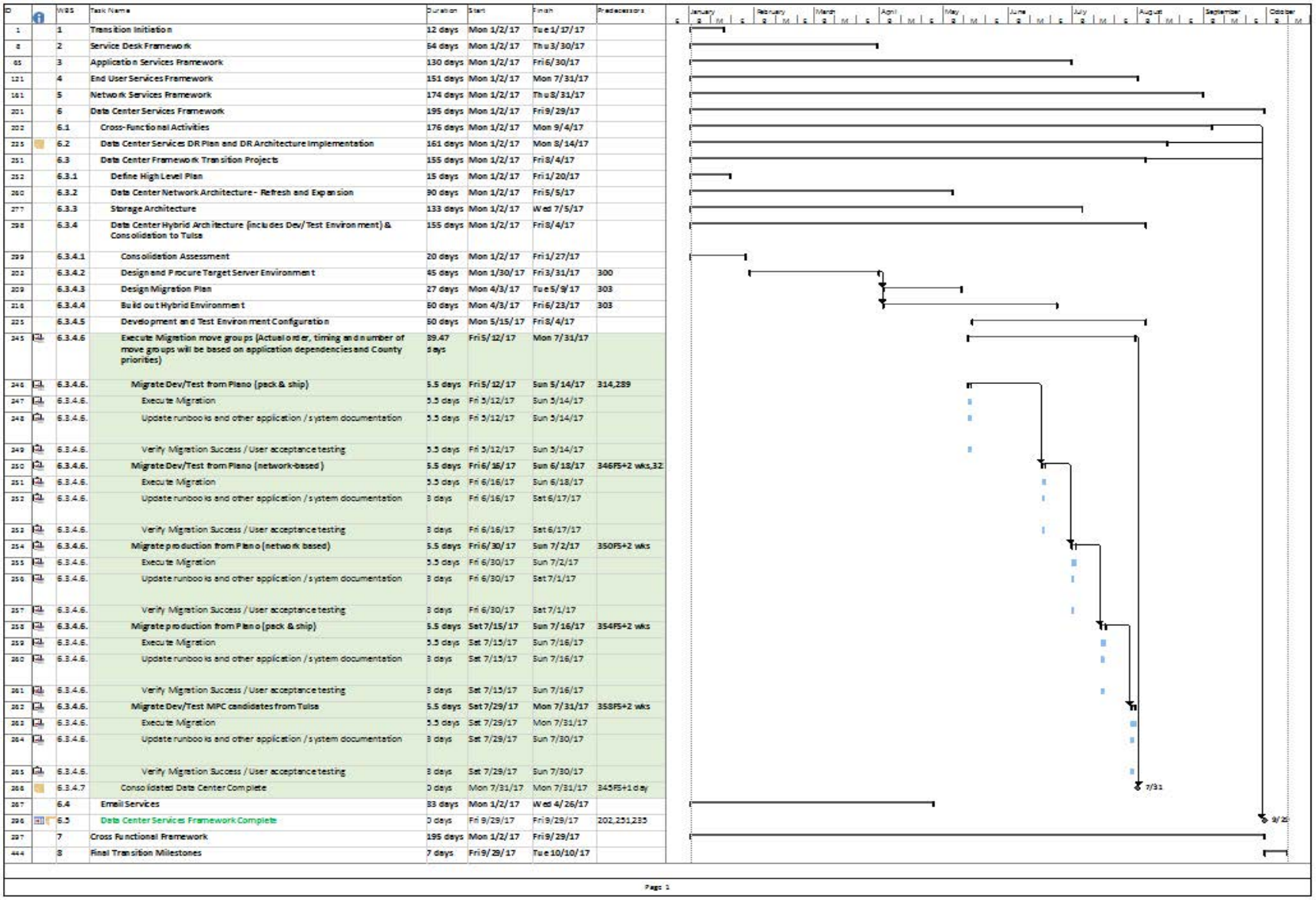
Design Migration Plan. During the design phase we also identify move groups that will organize the servers according to application dependencies, and incorporate other critical factors such as the change "freeze" periods, allowable maintenance windows, and other business priorities. The intent is to 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.

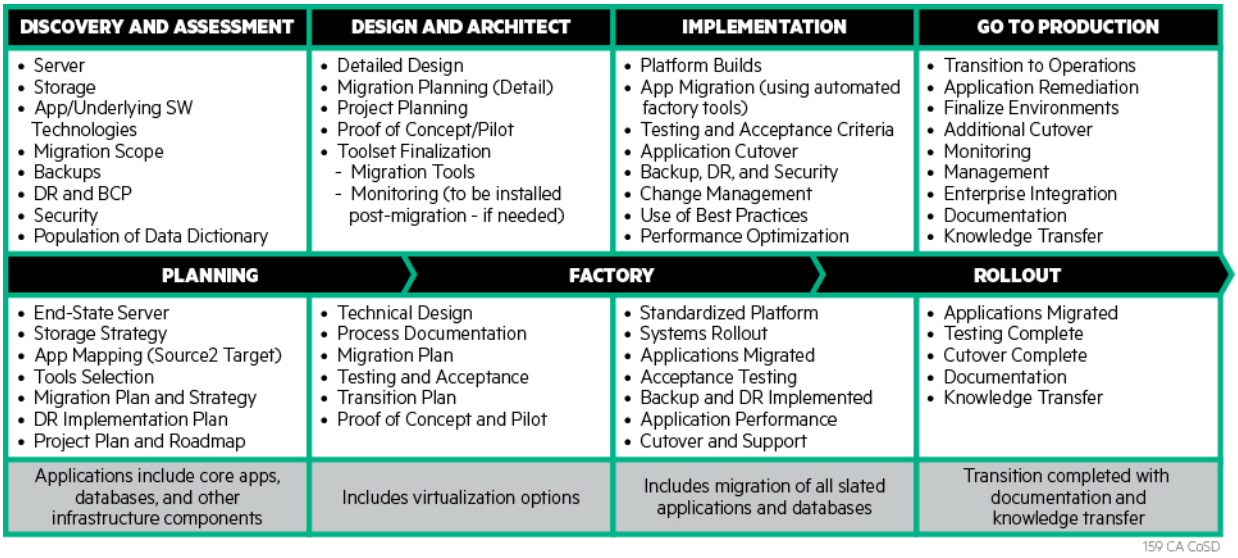
Figure 163. Draft Migration Plan Activities



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	
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	
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.

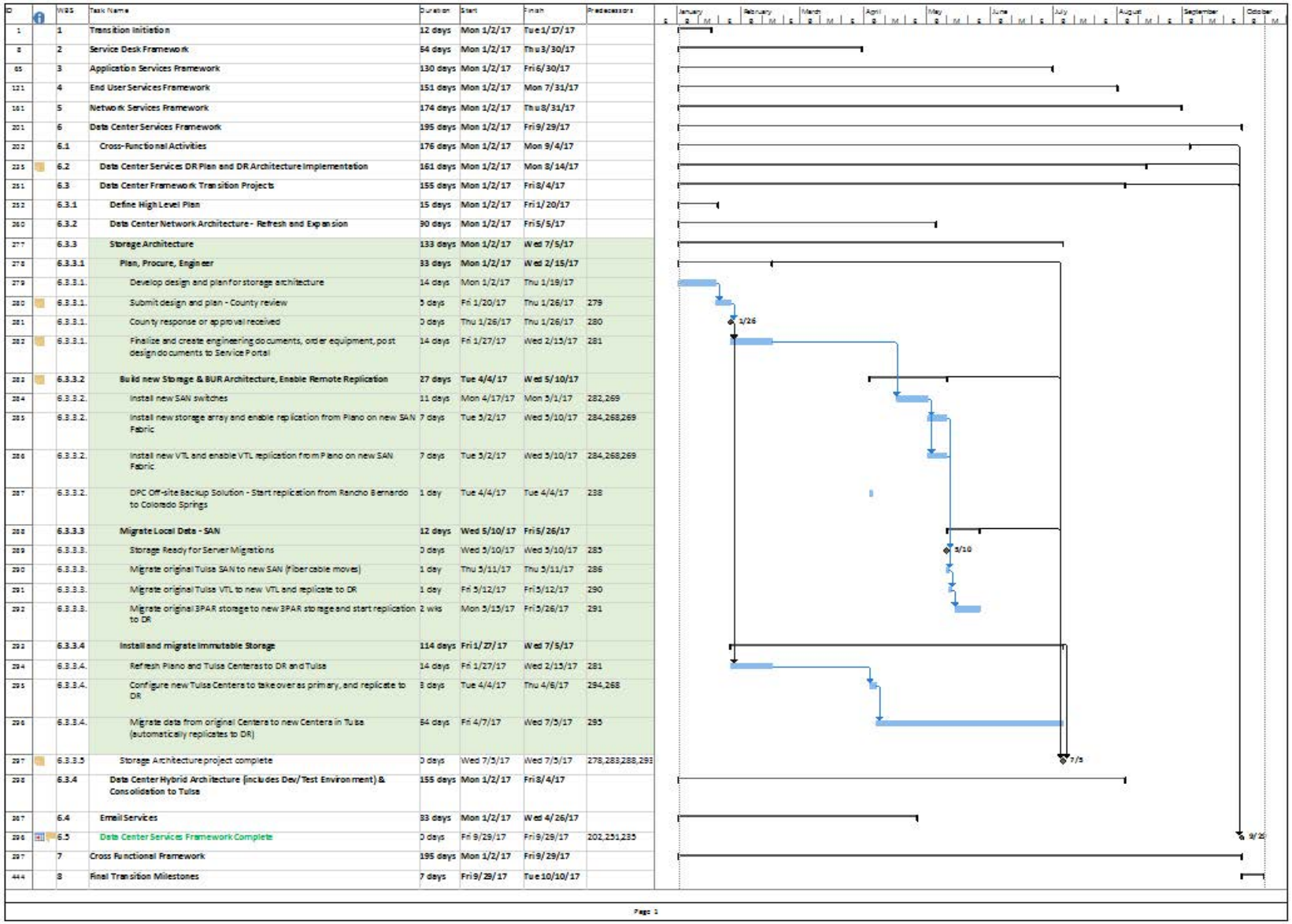
Build New Storage and Backup Architecture, Enable Remote Replication. Once hardware is received, we will begin the build process. We will install the new SAN switches, storage, and VTL in Tulsa, configure and test the environment, and begin the process of replicating data from the current Plano array 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:

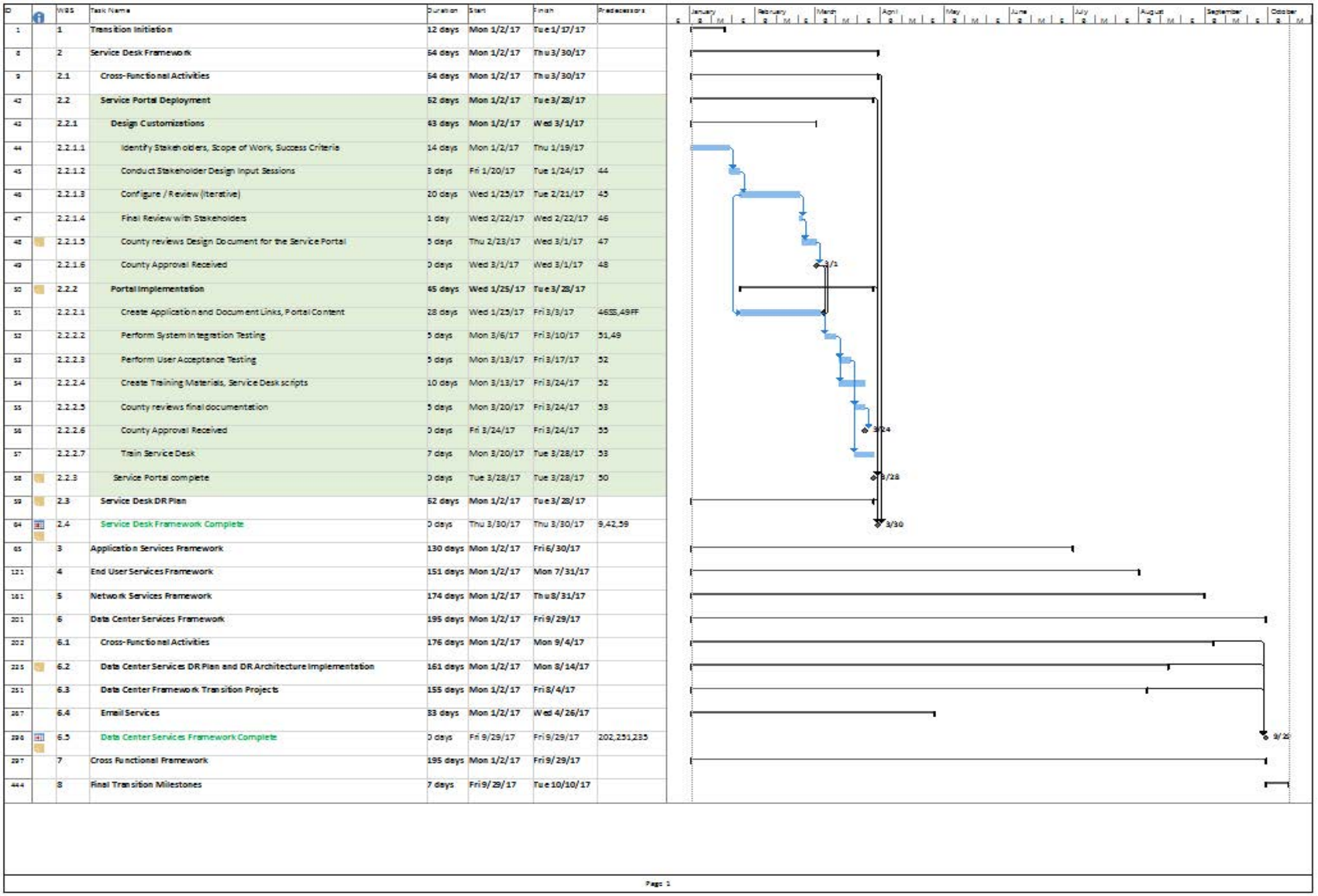
- County branding and "look-and-feel" elements on the front page (tiles, menus, links)
- Use of banners and splash pages
- Identification of user roles to be configured, to determine which groups have access to the various types of information
- Integration with Active Directory for Single Sign-on and 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:

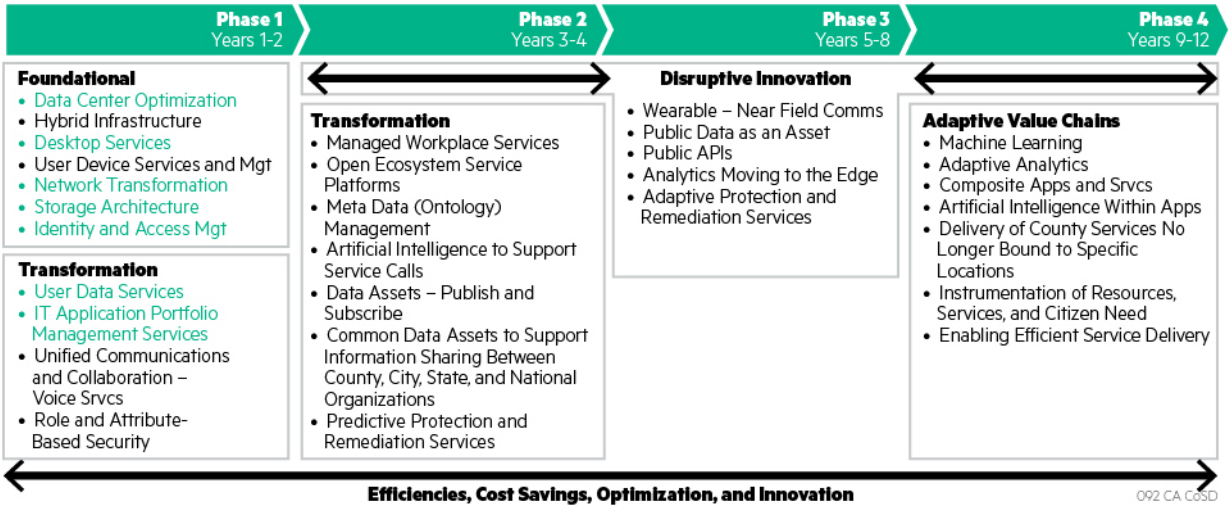
- **Enable citizen engagement (digital first) –** The County has recognized a growing preference among citizens to interact with the government online, at a time and place that is convenient for them, and they expect their experience to mirror that of the private sector. Tools, functions, capabilities, 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

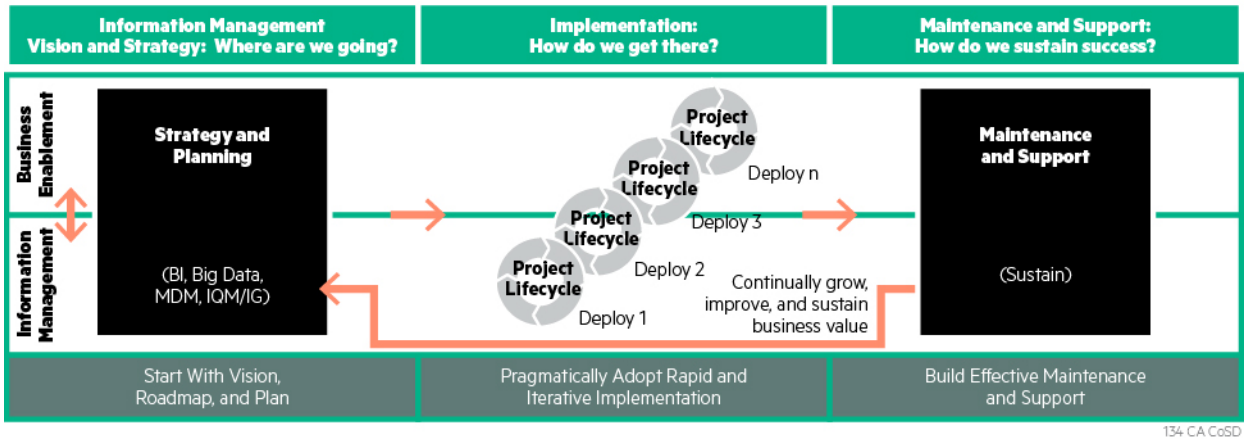
We are committed to making certain that transformation continues in the future, after successful completion of the identified transition and transformation projects. We will provide leadership and oversight for transformational projects through an Enterprise Architecture (EA) governance process that 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.

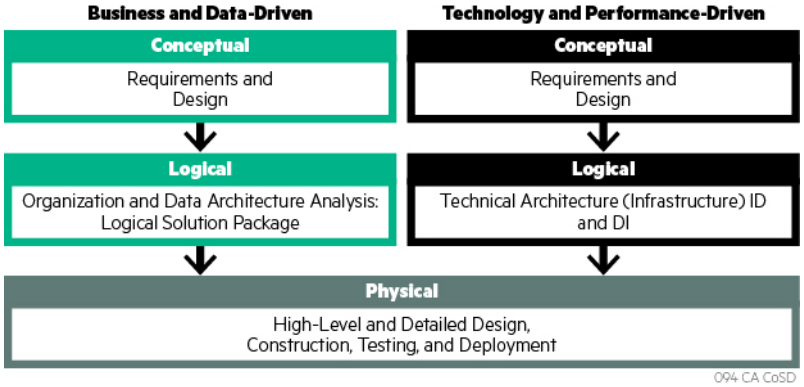
Table 85. Purpose and Key Benefits of each TIM Phase

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

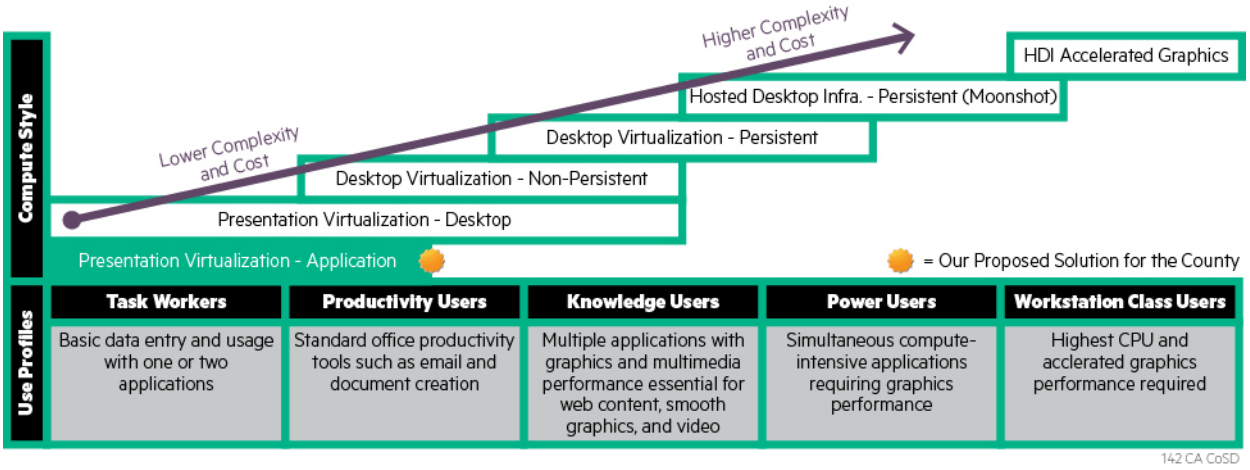
We assume High Concurrency of end users, meaning that for the most part, multiple users will be accessing the application(s) at the same time.

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.

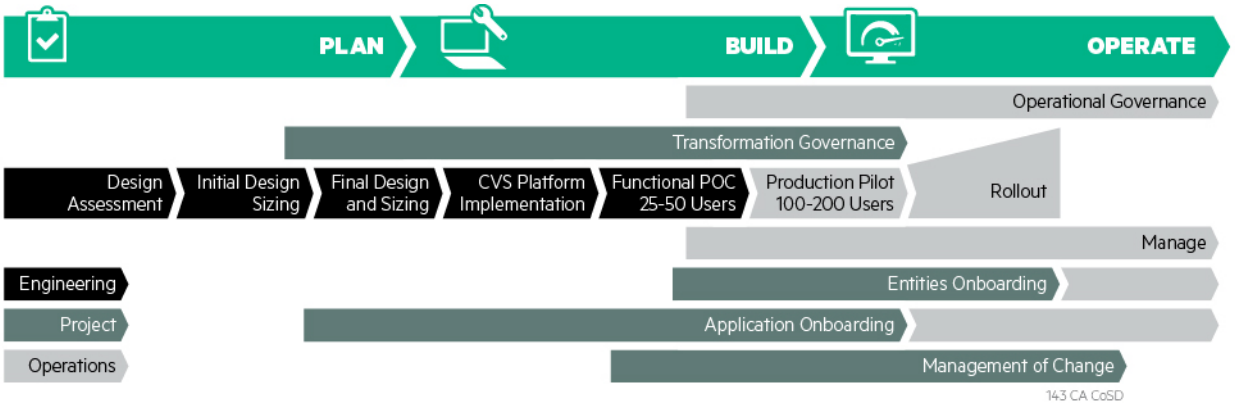
Risk Considerations: The introduction of client virtualization changes the way users perform their work and is therefore considered disruptive. Failed first attempts to introduce users to client virtualization result in roll-out delays, onboarding program rework and reintroduction to users which is costly, 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

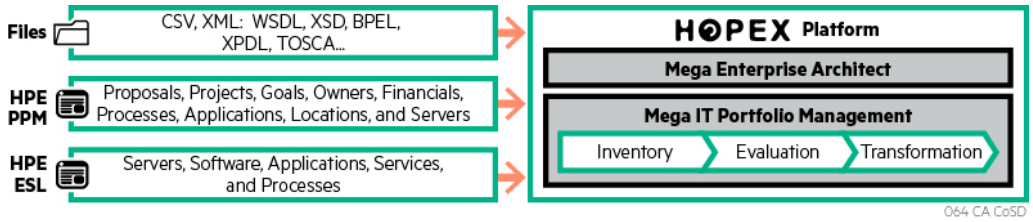
Key considerations for this transformation project require selecting a tool suitable for meeting the criteria listed below. These criteria are based on the initial list of items contained in Exhibit KK, and derived from the requirements.

- 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

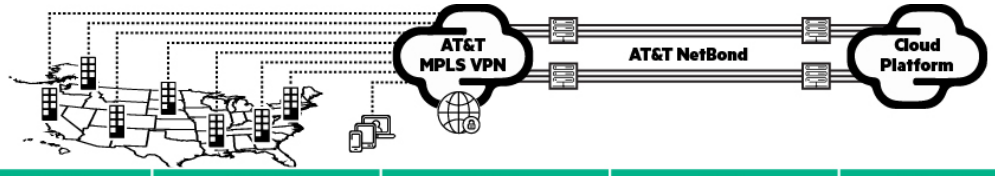
As cloud-based services mature and become more viable for Government use, we are positioning the County's network perimeter to enable seamless, secure, and performance-assured integration for cloud providers. AT&T will build a geo-redundant core network foundation to enable this shift in services, leveraging 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.

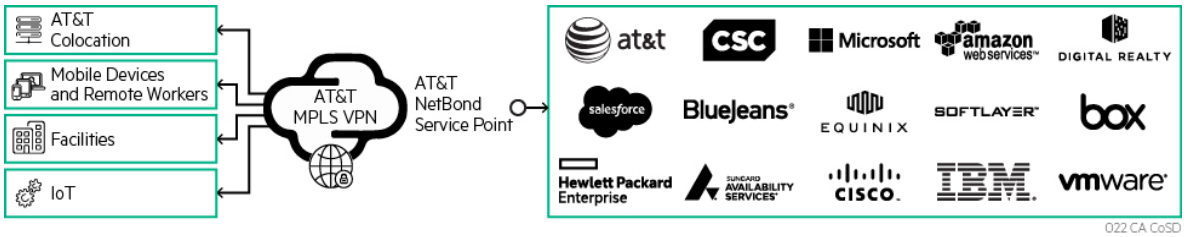


Figure 175. Security Benefits of AT&T NetBond

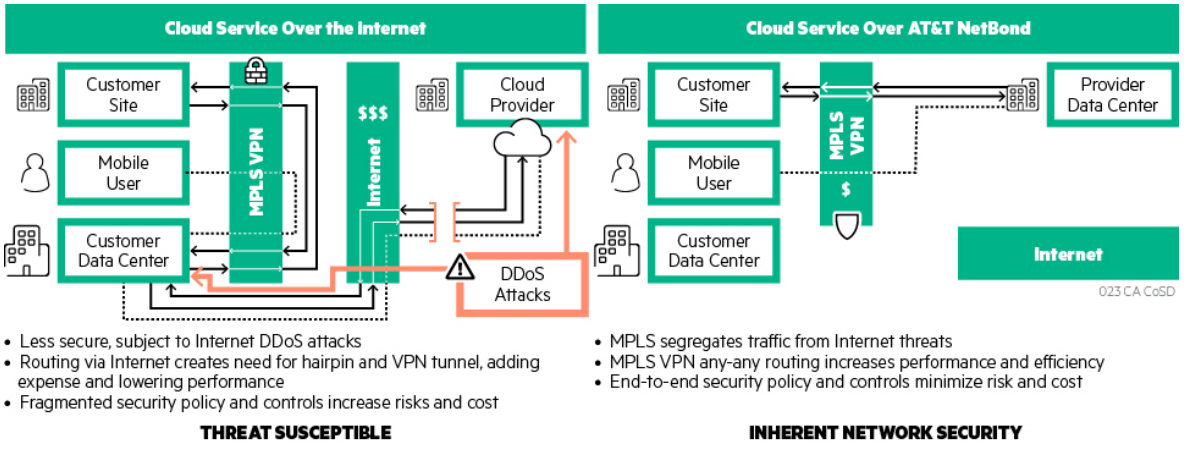
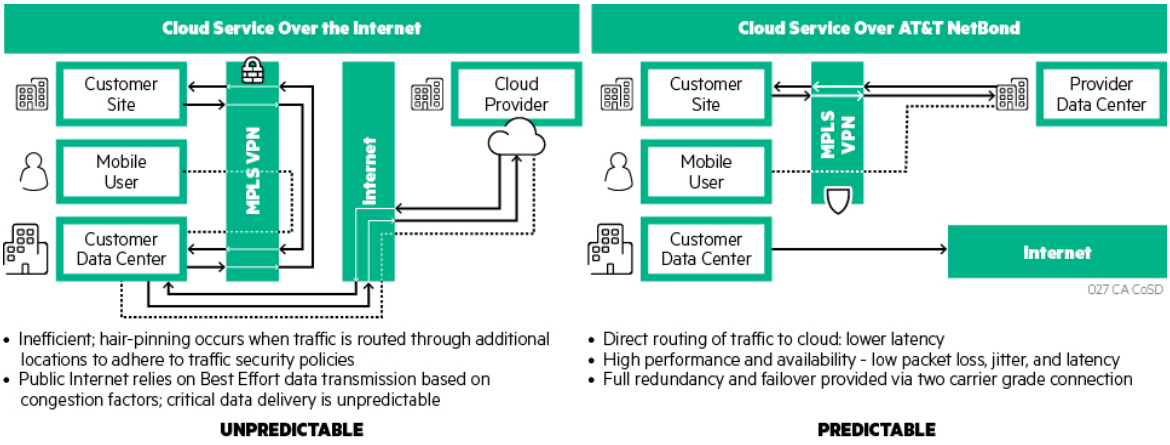


Figure 176. Performance Benefits of AT&T NetBond



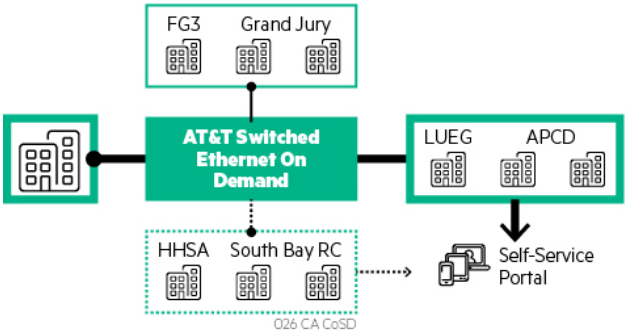
Migration to AT&T Switched Ethernet with Network on Demand

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



Fast Installation
Days in current fiber-enabled buildings

Dynamic Bandwidth
14 speeds with 5 CoS options

Flexible Deployment Models
Interconnect with existing AT&T Switched Ethernet; order services outside of current fiber footprint

Inter-LATA
Interconnect sites that reside in different cities and states

Digital Experience
Self-service portal to securely add and configure services

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

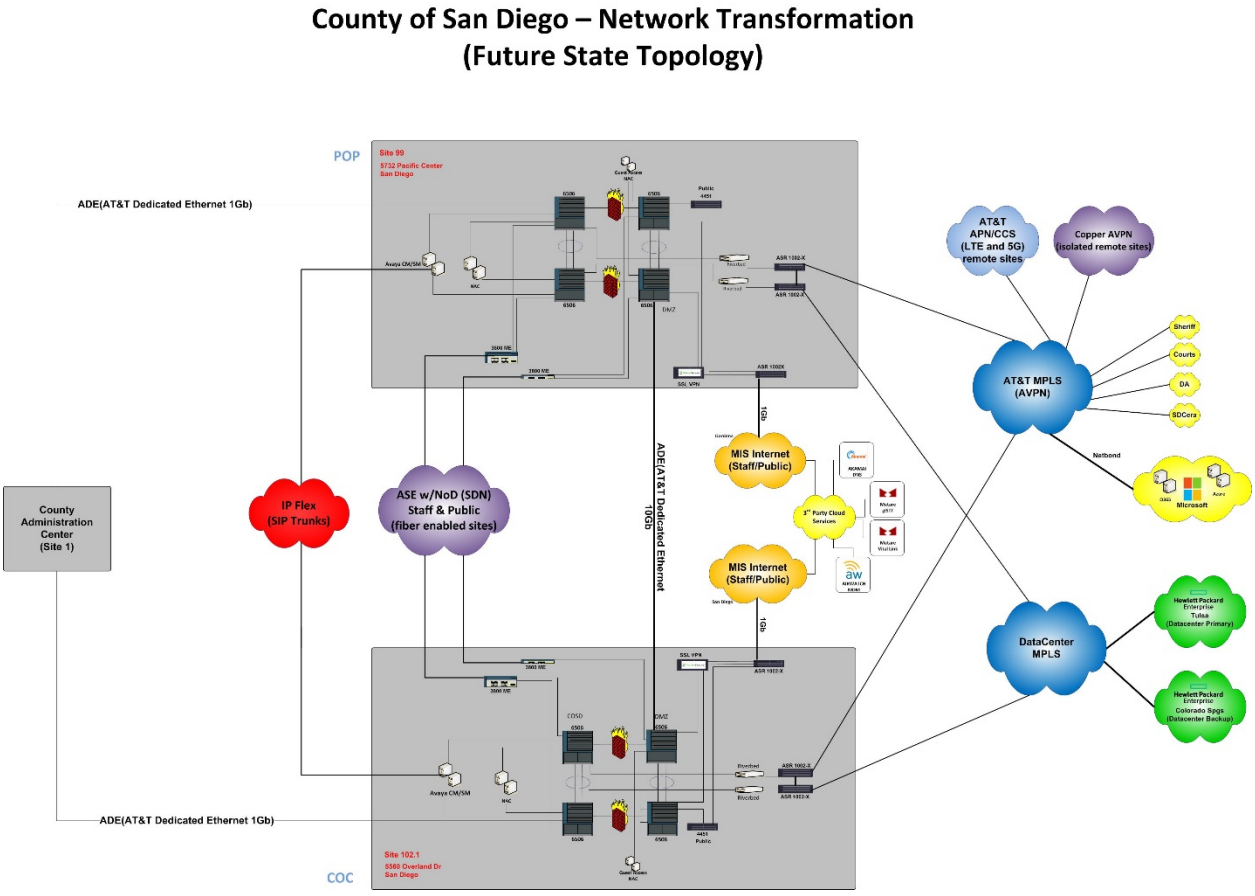
The standard Network on Demand design provides geo-redundant host circuits, however from the last Central Office, this diversity is reduced to a single fiber pathway to the remote site. The redundancy design will involve provisioning a redundant circuit with diverse fiber path and infrastructure from 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

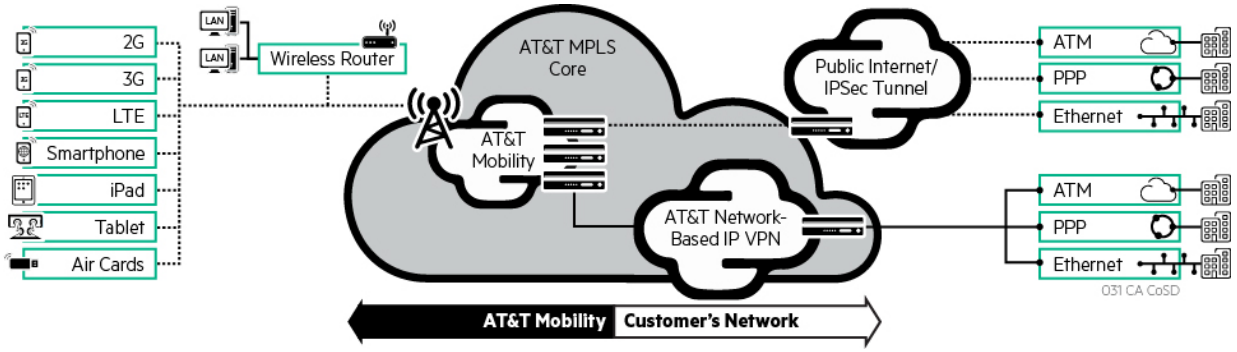
As identified earlier, T1 transport utilizing legacy TDM based connectivity, will be targeted for migration to ASE with NOD where possible. However, where fiber is not available without prohibitive construction cost, AT&T will evaluate products such as copper-based AVPN that provides transport redundancy 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.

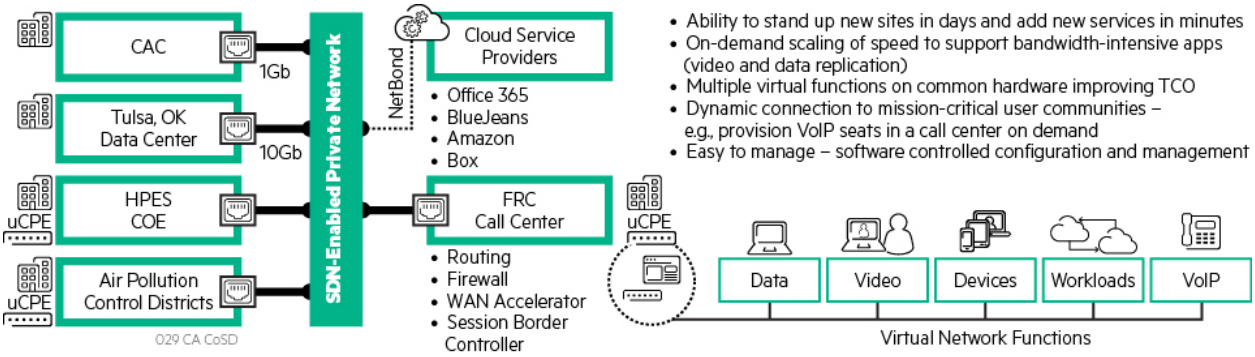
Figure 179. Commercial Connectivity Service – Enterprise Secure Connectivity using AT&T's LTE Mobile Network



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.

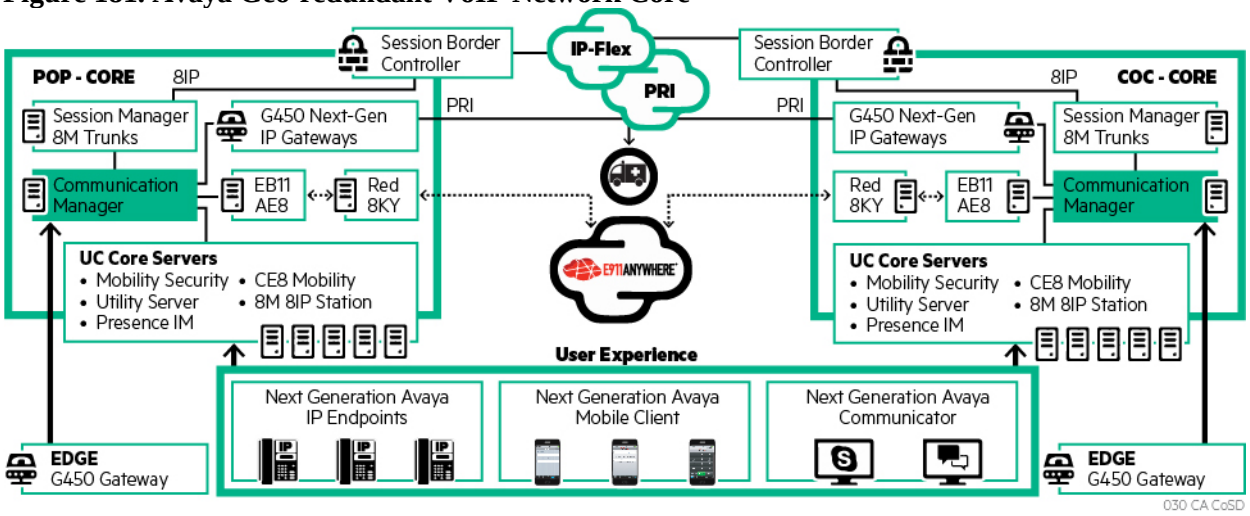
This highly available architecture will provide seamless failover between the COC and POP, with no single point of failure of the Core VoIP gateways. The proposed architecture not only will provide centralized management between the two "Core" locations—POP and COC—but will also provide access to the 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.

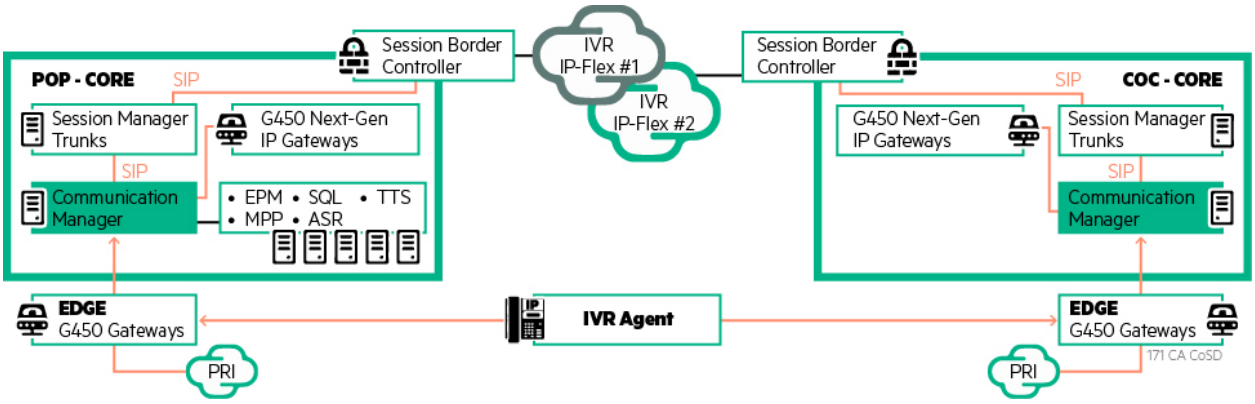
Interactive Voice Response (IVR) Transformation

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.

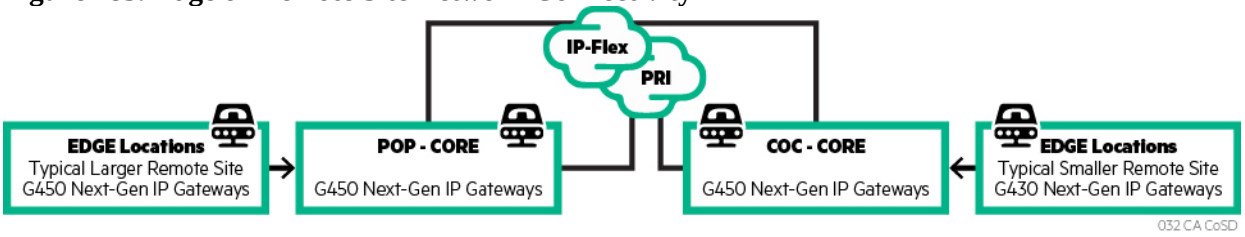
Figure 182. Avaya's Experience Portal leverages geo-redundant communication managers and redundant SIP trunking for inbound and outbound contact center traffic.



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.

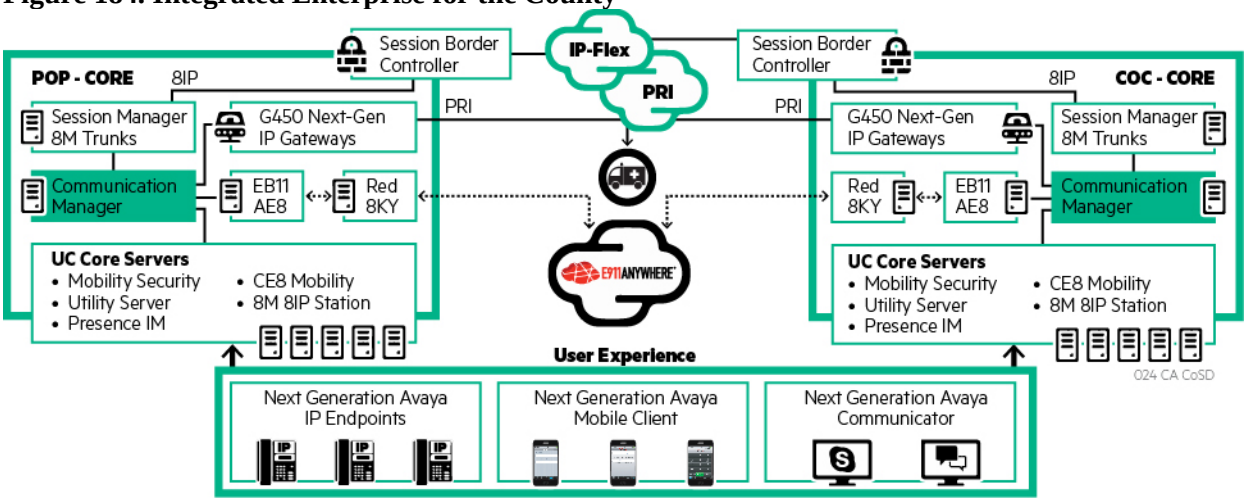
If a phone number is on an enterprise web page, Collaboration Services will take this number, access Active Directory, and pull down additional information for this user. This information is displayed on a contact card. The contact card is also populated with icons that enable the user to send an IM 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

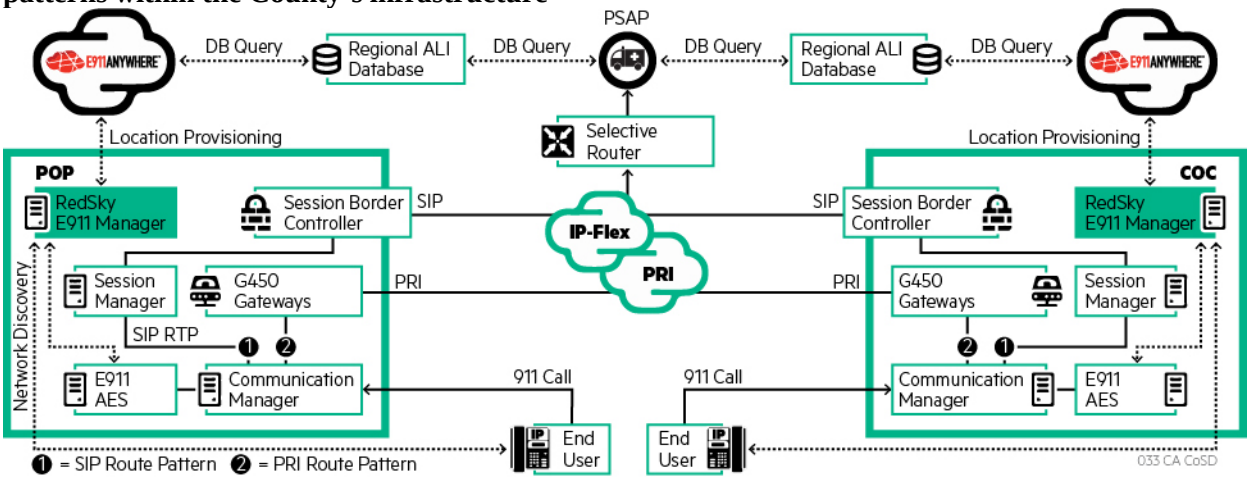
Enhanced 911 (E911) is an important complementary solution to an enterprise Voice over Internet Protocol (VoIP) deployment. As call control is converged into the geo-redundant voice core infrastructure and VoIP is enabled at the telephone set, there is an imperative to provide emergency responders with 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:

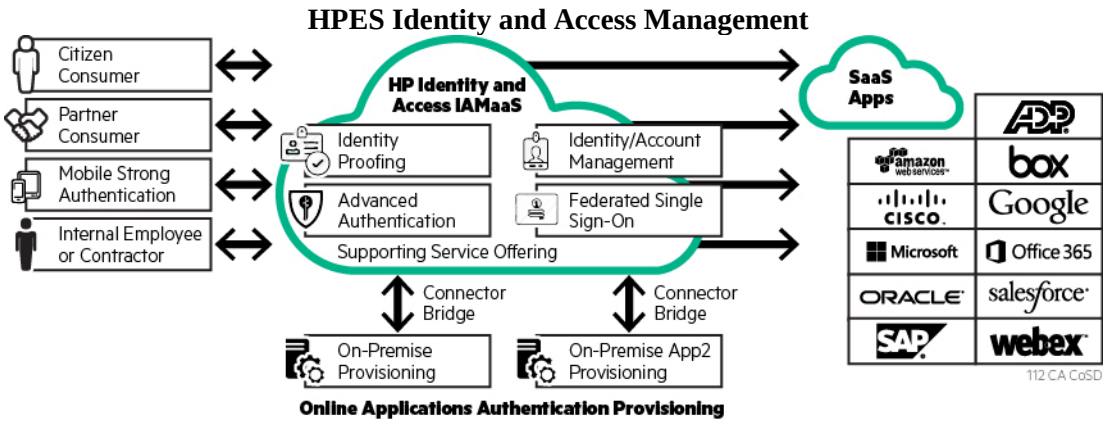
- The existing Oracle IDAM technology platform as its core
- Microsoft Active Directory Federation Services (ADFS)
- HPE's IAMaaS to enable the federation services where the County is acting as service provider and identity provider.

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.

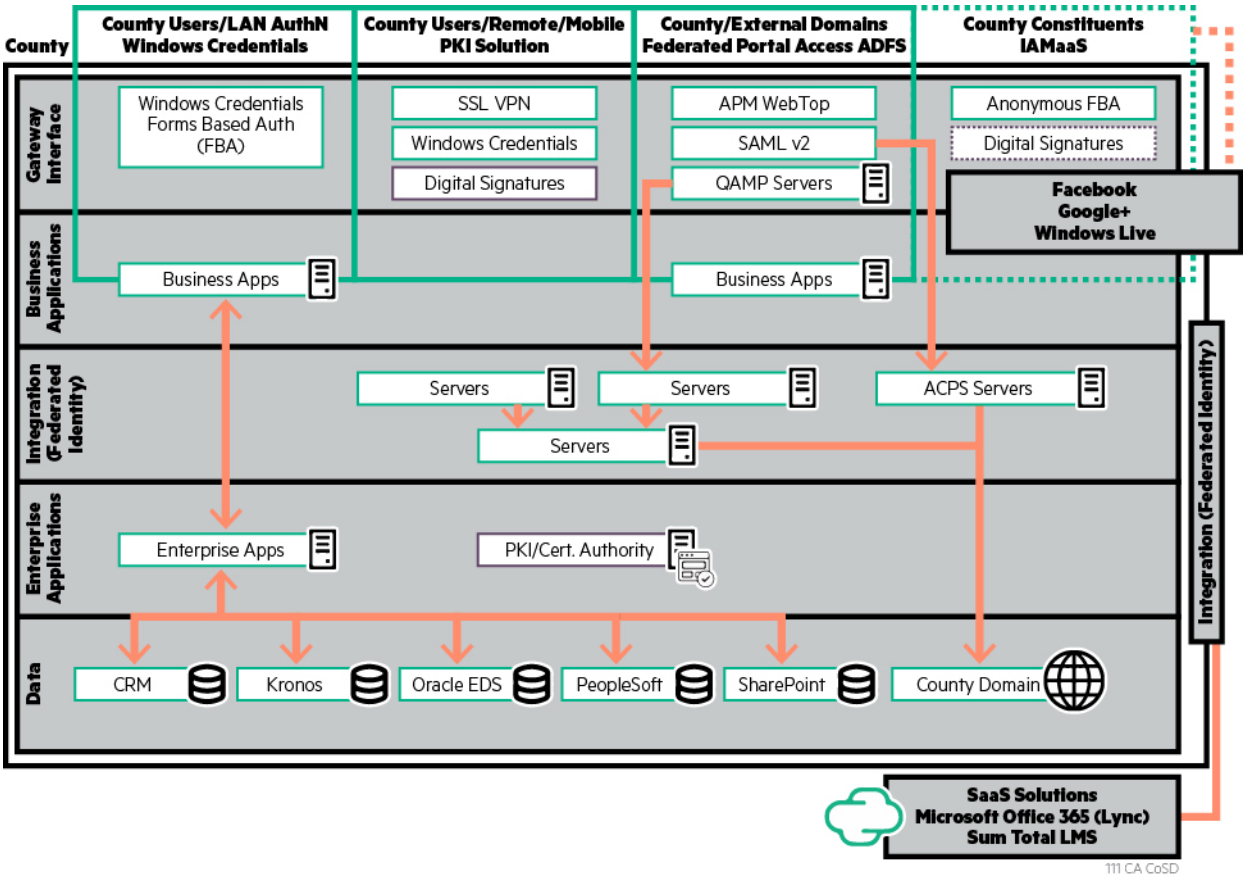
Figure 189 below depicts the overall view of the IDAM solution and how Oracle, ADFS, and the HPE's IAMaaS will work together to provide identity federation. As seen in the figure, the core elements of the IDAM solution will work together to enable seamless federation between the County and third-party 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

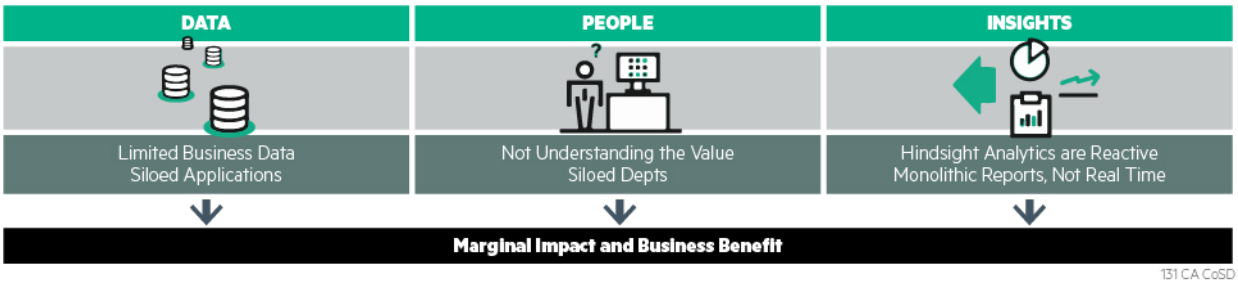
- Key Considerations and Potential Alternative Approaches

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.

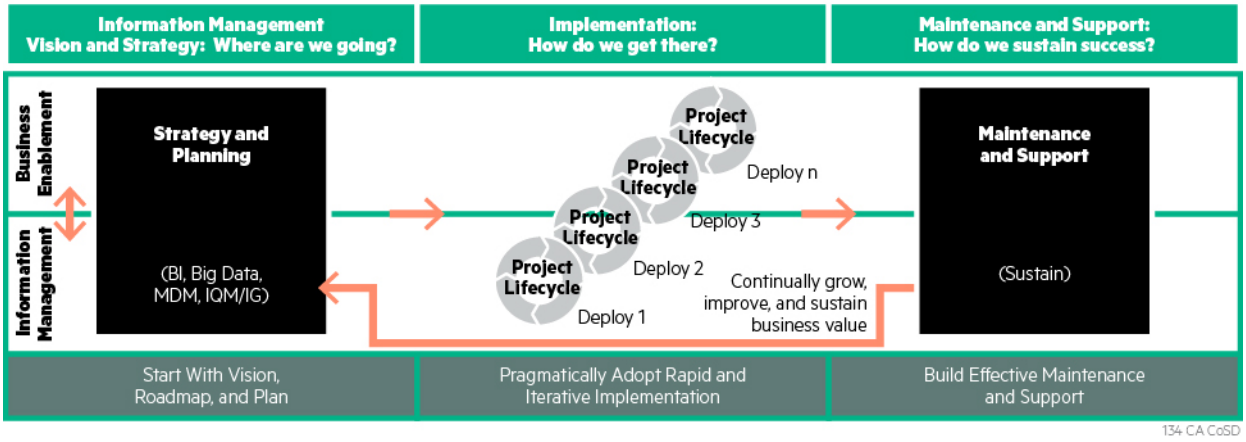
- Solution Summary & Rationale – Description of proposed solution to meet the requirements and the rationale for choosing this solution rather than alternative approaches. Include timing and risk considerations, key dependencies and milestones

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.

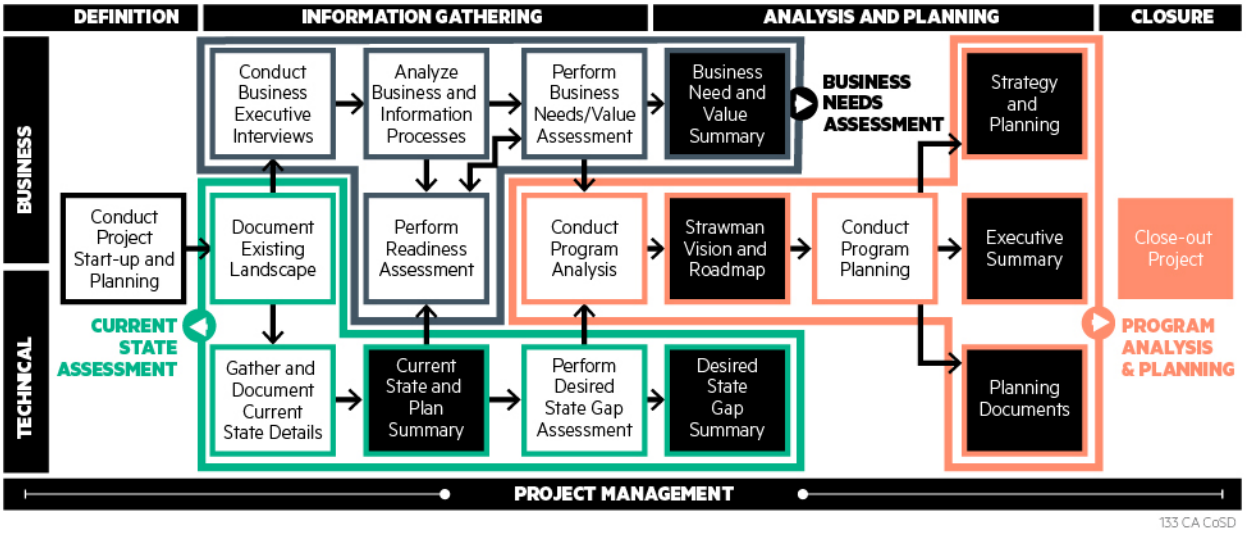
- Resource and Facility Approach Summary – Proposed deployment plan for resources and use of facilities

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.

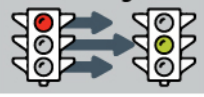
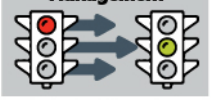
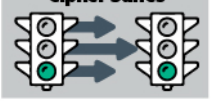
The Security Requirements Gap Analysis is based on:

- 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 C6SD

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.

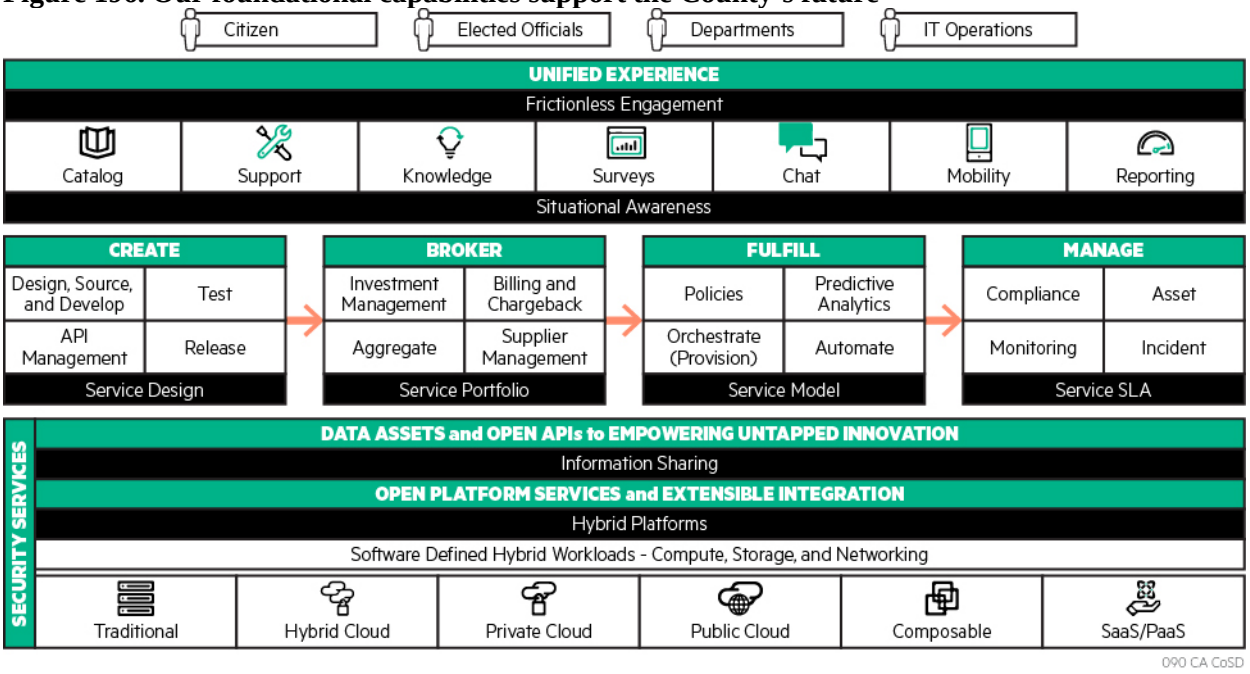
None.

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.

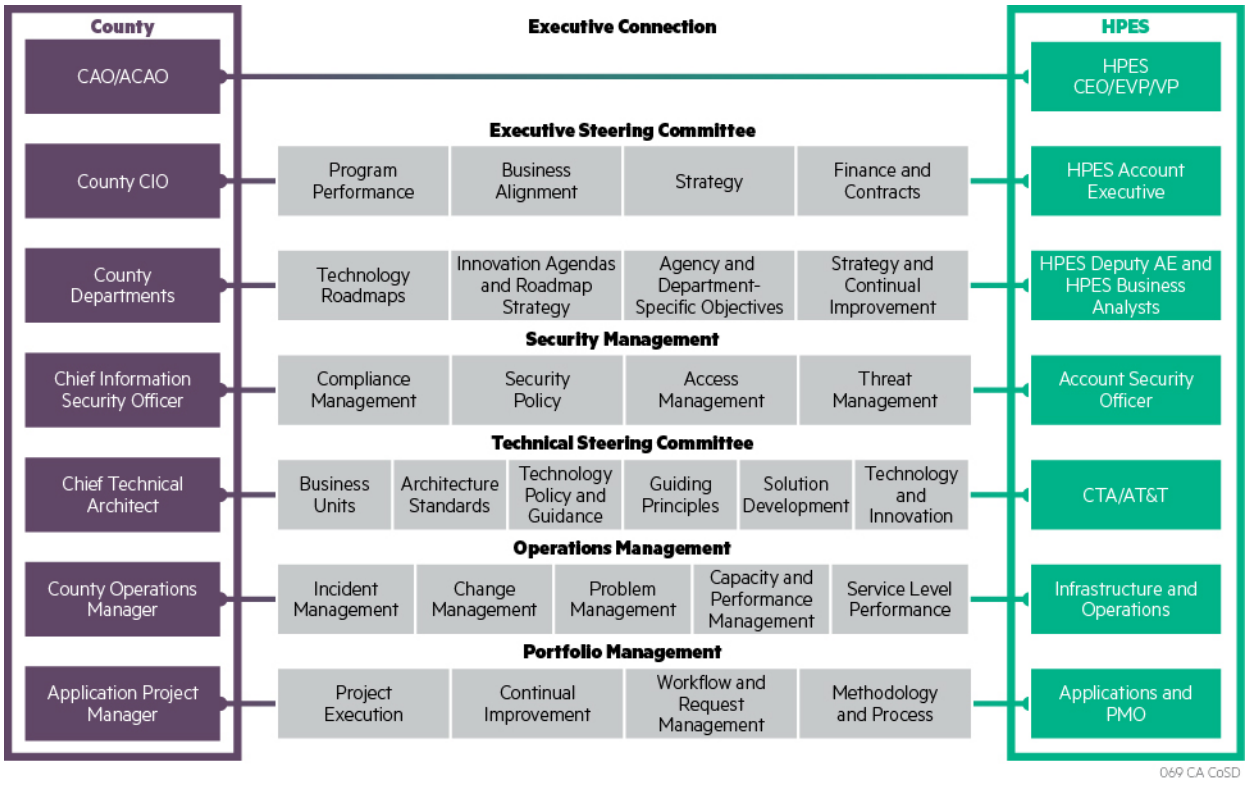
KEY POSITIONS	PROPOSED NAMED INDIVIDUAL
Account Executive	Cathy Varner
Deputy Account Executive	Laura Floyd
Enterprise Service Delivery Manager (SDM)	Kathleen Barghols
FG3 Service Delivery Manager (SDM)	John Steed
CSG Service Delivery Manager (SDM)	Frank Krone
HHSA Service Delivery Manager (SDM)	Sandra 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.

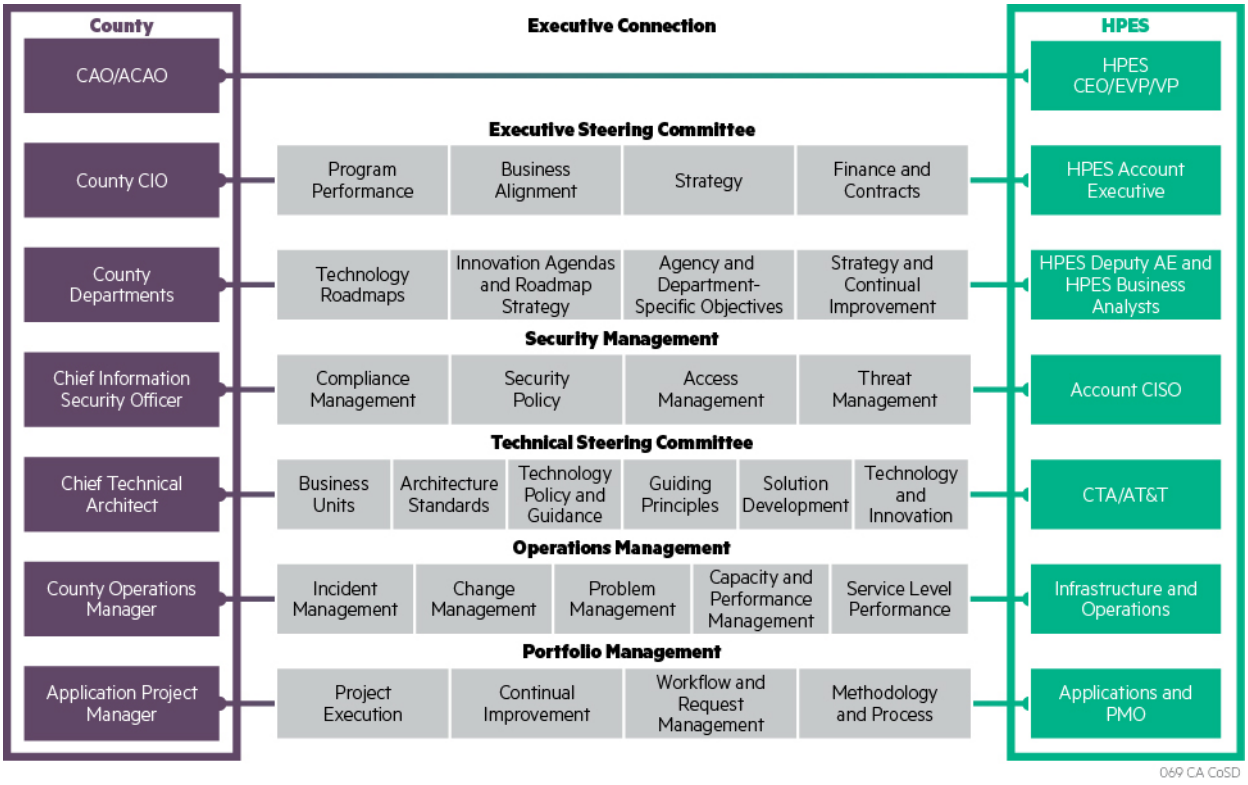
KEY POSITIONS	PROPOSED NAMED INDIVIDUAL
Account Executive	Cathy Varner
Deputy Account Executive	Laura Floyd
Enterprise Service Delivery Manager (SDM)	Kathleen Barghols
FG3 Service Delivery Manager (SDM)	John Steed
CSG Service Delivery Manager (SDM)	Frank Krone
HHSA Service Delivery Manager (SDM)	Sandra 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.