



Problem Resolution Report



CoSD Contract no. 537863
Data Loss Prevention
HP/CoSD-121

October 5, 2015

Summary:

In accordance with the provisions of the IT and Telecommunications Service Agreement by and between the County of San Diego ("County") and HP Enterprise Services, LLC ("HP" or "Contractor") (hereinafter collectively referred to as "the Parties") originally dated January 24, 2006 and restated on April 5, 2012 ("the Agreement"), agreement is reached on the date shown above.

Issue or Problem:

The County is requiring a comprehensive, secure and easy-to-use solution to monitor real-time traffic and extends visibility and control over where confidential data is allowed to migrate; who is using it; how it is being used; where it is being transferred; and what real-time action is taken to prevent data loss at the endpoint or via the web. The solution must allow security administrators to either block or monitor and log files that present a potential policy breach. The solution must enable the creation of policies that allow full visibility of content traffic and contain data loss at the endpoint or via the web without restricting device usage.

Resolution:

1. Contractor will provide County with a comprehensive Data Loss Prevention (DLP) Solution using the Websense Web Security Anywhere (Websense) software and related DLP tools. Websense is a hybrid security gateway with both appliance and cloud security defenses that provide protection against data loss for both onsite and remote workers. Websense DLP tools will provide County the capability to monitor traffic over the web channel and at endpoints, enforce County DLP policies, and receive notification of policy violations via reports and automated email notifications. Remote users are included in the DLP solution via web content filtering function.
2. DLP Solution will have a fixed monthly Resource Unit (RU) Fee of \$3,885.94. This RU will be allocated to County departments using the approved Cross Functional allocation method. This RU Fee covers support and maintenance of the DLP solution for up to 14,000 client endpoints (e.g. desktops, laptops and tablets) that are in scope for licensing and maintenance. This includes support for a maximum of three 'out of the box' reports on security incidents and a maximum of three policies implemented as part of the DLP project.



Problem Resolution Report



CoSD Contract no. 537863
Data Loss Prevention
HP/CoSD-121

3. The DLP Solution RU Fee will not include the following:
 - Break fix for incident support activities. Such activities will be charged through an NDWR at the Infrastructure Security Analyst rate of \$127/hour.
 - Forensic activity (i.e. monitoring, analysis, investigation etc.) by Contractor. County 'policy managers' will be responsible for responding to and addressing County employees' questions regarding alerts and associated
 - Physical monitoring of the console for policy violation alerts and investigation of policy violation alerts by Contractor. County 'policy managers' will be responsible to address CoSD employee questions regarding alerts and associated CoSD policy as well as taking action on the alerts.
 - Integration of DLP Solution with any mobile device (i.e. Blackberry, iPhone, iPad, Android, etc.) whether County or employee owned.
 - Content other than URL web based traffic though the Websense Gateway or Cloud as well as data from the endpoint.
 - Customization of the out of the box reports provided by the application
 - Integration with other systems such as Security Information and Event Management.
 - System and hardware redundancy
 - Any additional Desktop Services support for upgrades or maintenance. County will be responsible for funding any changes related to the MSI scripts, including new releases, upgrades, etc.

4. Section 5.7 – Data Loss Prevention Services is hereby added to Schedule 4.3 – Operational Services, as per Attachment 1 to this PRR.

5. Schedule 16.1, Fees, Exhibit 16.1-5 – shall be supplemented by the addition of a Data Loss Prevention Resource Unit, as per Attachment 2 to this PRR.

The resolution of the issue or Problem as described in this Problem Resolution Report shall govern the Parties' actions under the Agreement until a formal amendment of the Agreement is implemented in accordance with the terms of the Agreement, at which time this Problem Resolution Report shall be deemed superseded and shall be null and void.

All other terms and conditions of the Agreement remain unchanged and the Parties agree that such terms and conditions set forth in the Agreement shall continue to apply. Unless otherwise indicated, the terms used herein shall have the same meaning as those given in the Agreement.



Problem Resolution Report



CoSD Contract no. 537863

Data Loss Prevention

HP/CoSD-121

IN WITNESS WHEREOF, The Parties hereto, intending to be legally bound, have executed by their authorized representatives and delivered this Problem Resolution Report as of the date first written above.

COUNTY OF SAN DIEGO

HP ENTERPRISE SERVICES, LLC

By: *John M. Pellegrino*

By: *Laura Floyd*

Name: John M. Pellegrino

Name: Laura Floyd

Title: Director, Department of Purchasing
and Contracting

Title: Director, SLED

Date: _____

Date: 10/5/15

5.7 Security Services

5.7.1 Security Services Overview

The Security Services component of Network Services includes the hardware, software, and services provided to maintain network security, including:

- Protection from unauthorized devices, software or users
- Protection from unauthorized access to, or use of, the network and networked assets
- Firewall services
- Intrusion detection and reporting
- Security monitoring
- Security architecture services
- Data protection
- Prevention of malicious code entry into the network
- Data loss prevention services for traffic via web channels for onsite and remote workers as well as traffic from the client endpoint for up to 14,000 endpoints

5.7.2 Security Services High Level Requirements

5.7.2.1 Develop and maintain flexible security architecture

5.7.2.2 Provide protection from unauthorized use of, or access to, the County's network and networked assets.

5.7.2.3 Protect all data residing on the network from intrusion, destruction or compromise.

5.7.2.4 Contractor shall refresh Security Services assets on a 5 year refresh schedule, 20% per year and at a County-approved deployment schedule that will minimize disruption and reduce risk. Refreshes of Security Services assets may include upgrades of active/intelligent components that provide significant upgrades in functionality and performance, if approved by the County.

5.7.3 Security Services Environment

The following further describes and scope of Security Services elements to be supported by Contractor and with which Contractor shall comply.

5.7.3.1 Intra-County and Public Network Access Security Services

This includes all the Security Services associated with network usage and services for County end-users and the public, including Security Services for:

5.7.3.1.1 County data jacks

5.7.3.1.2 County voice jacks

5.7.3.1.3 Remote access

5.7.3.1.4 Access to and from the County network through the Internet

5.7.4 Security Services Requirements, Roles and Responsibilities

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with Security Services.

Security Service: Plan, Build and Operate Requirements, Roles and Responsibilities		
Plan Requirements, Roles and Responsibilities	Contractor	County
1. Produce and submit recommendations for Security architecture	X	
2. Review and approve recommendations for Security architecture		X
3. Produce and submit plans for monitoring and managing access to the County Intranet	X	
4. Review and approve plans for monitoring and managing access to the County Intranet		X
5. Produce and submit plans that provide security to physical and logical devices connected to the network	X	
6. Review and approve plans to include the provision and support of methods that provide security to physical and logical devices connected to the network		X
7. Produce and submit recommendations on firewall policies that comply with County policy	X	
8. Review, approve and identify firewall policies that comply with County policy		X
9. Produce and submit recommendation of Security Services assets refresh or upgrade plan on a yearly basis	X	
10. Review and approve recommendations on Security Services assets refresh or upgrade plan		X
11. Produce and submit recommendations for improved network security	X	
12. Review and approve recommendations for improved network security		X
13. Produce and submit recommendation of policies for security vulnerability & penetration testing	X	
14. Review and approve policies for security vulnerability & penetration testing		X
15. Produce and submit plans for Security Services asset updates or patches	X	
16. Review and approve plans for Security Services asset updates or patches		X
Build Requirements, Roles and Responsibilities	Contractor	County
17. Design, test and implement approved Security architecture	X	
18. Design and implement monitoring and managing access plans as approved	X	
19. Design, test and implement plans to secure network attached devices	X	
20. Design, test and implement approved firewall policies	X	
21. Design, test, implement and report Security Services assets refresh or upgrade	X	
22. Review and approve reports for Security Services assets refresh or upgrade		
23. Design and implement approved recommendations for improving network security	X	
24. Design and implement approved policies for security vulnerability & penetration testing	X	

Security Service: Plan, Build and Operate Requirements, Roles and Responsibilities		
Plan Requirements, Roles and Responsibilities	Contractor	County
25. Design, test and implement updates or patches approved for Security Services assets	X	
26. Enable technologies that use a centralized authentication database for remote County employees, contractors and agents using VPN and will deploy new systems capable of interfacing with single-sign-on authentication services	X	
27. Deploy a Security Information Management System (SIMS) for aggregation and centralization of incident alerts and correlation and provide SIMS information to the County through online access	X	
Operate Requirements, Roles and Responsibilities	Contractor	County
28. Provide support, including break-fix, for all Security Services assets	X	
29. Provide 24x7x365 security monitoring services including a Security Operations Center (SOC), IDS/IPS infrastructure and intranet/Internet firewalls	X	
30. Provide Services in conformance to firewall policies and requirements	X	
31. Provide reporting on security testing results	X	
32. Provide initial review of security Break-Fix incidents and the determination if escalation, including to County Information Security, is warranted except for incidents related to Data Loss Prevention and web content filtering for off premise users.	X	
33. Provide standardized End-user operations and capabilities and also custom reports regardless of the End-user's location and/or department	X	
34. Identify and remove from the network any malicious-code (malcode) infected System	X	
35. Identify and provide countermeasures for malcode attacks (i.e., both prevention and remediation)	X	
36. Block unauthorized party access and provide notification of unauthorized access attempts	X	
37. Encrypt (and prioritize) all County traffic that uses public MPLS network transport facilities (such as OPT-E-MAN or DSL) through the engineering and implementation of generic routing encapsulation (GRE) VPN tunnels (e.g. 256-bit Advanced Encryption Standard (AES) key)	X	
38. Provide technical expertise for security audits	X	
39. Collect all logs and review all Break-Fixes reported by all other security services (e.g. NIPS, HIPS, penetration testing, and firewall) with the exception of data loss prevention and web content filtering for off premise users	X	
40. Maintain log files in accordance with County policies and MASLs	X	
41. Provide security reporting	X	
42. Provide fraud prevention, detection and reporting	X	
43. Provide, control, monitor, and maintain security encryption interface at the data network level	X	
44. Provide security devices on supported PBXs, voicemail systems, and other appropriate adjunct remote administration ports	X	
45. Implement security violation notification. This function notifies a designated station/End-user/administrator when a hacker attempts to breach System management	X	

Attachment 1 to PRR 121 – Data Loss Prevention

Security Service: Plan, Build and Operate Requirements, Roles and Responsibilities		
Plan Requirements, Roles and Responsibilities	Contractor	County
46. Conduct security perimeter vulnerability assessments and annual penetration testing	X	
47. Define data loss prevention policies		X
48. Implement, support and administer County provided data loss prevention policies	X	
49. Monitor, investigate and resolve alerts associated with data loss prevention		X
50. Provide standard (out of box) reporting for data loss prevention	X	
51. Enable and support automated notification of potential data loss prevention policy breaches	X	
52. Enable automated blocking of data according to County policy	X	
53. Provide system administration for data loss prevention	X	

Attachment 2 to PRR 121 - Data Loss Prevention

Exhibit 16.1-5

Resource Unit	Schedule 4.3 Cross-Reference/Service Framework Component **	Unit of Measure	Pricing	Resource Unit Fee (90% to 110% band)	Baseline Volumes (per Contract Year)	(Resource Unit Fee) x (Baseline Volume)	Bundled Resource Unit	Resource Unit Fee (70% to 80% band)	Resource Unit Fee (80% to 90% band)	Resource Unit Fee (110% to 120% band)	Resource Unit Fee (120% to 130% band)	Measurement Methodology (Specific measurement on last day of Month of
Data Loss Prevention	Network Services - Security Services - Section 5.7	Month	Fixed Fee	\$ 3,885.94	12	\$ 46,631.28	N/A	N/A	N/A	N/A	N/A	N/A