



Problem Resolution Report
CoSD Contract No. 568996
Service Level 46 – Server Software Update
Revision
Peraton/CoSD – 135



Date: February 2, 2024

Title: Service Level 46 – Server Software Update Revision

PRR Number: 135

Summary:

In accordance with the provisions of the IT and Telecommunications Service Agreement by and between the County of San Diego (“County”) and Peraton Enterprise Solutions LLC (“Contractor” and hereinafter collectively referred to as “the Parties”) with the effective date November 15, 2016 agreement (“the Agreement”) is reached on the effective date shown below.

Issue or Problem:

Per Problem Resolution Report (PRR) 107, Service Levels 46-4 and 46-5 were modified and made effective April 2022 to better align with the tools and processes that were adopted to measure patching activities. Since the implementation of PRR 107, there continues to be challenges in meeting the patching cycle.

Resolution:

1. Parties agree to revise the Service Levels (SLs) 46-4 and 46-5 to a 60-day remediation cycle period and limit to critical and high vulnerabilities.
2. Parties agree that reporting for SL 46-4 and 46-5 per this PRR shall be effective March 1, 2024. Contractor shall have the opportunity to assess the revised SL following the execution of this PRR through to the effective date. During this assessment period, SL 46-4 and 46-5 shall remain zero weighted.
3. Parties agree to a redistribution of SL weighting affecting 46-1 through 46-5 and SL 48. The Service Level Weighting Table is revised effective March 1, 2024, for the following SL’s only:

Service Level ID	Framework	Service Level	Weighting
46	Data Center	46-1 – Server Software Update - Operating system patching and updates for Windows and Linux servers	2%
		46-2 – Server Software Update - Operating system patching for Solaris and AIX servers	
		46-3 – Server Software Update - Operating System Patching for Critical and Zero Day Vulnerabilities	1%
		46-4 – Server Software Update - Middleware patching for Production PAIDs	1.5%



Problem Resolution Report
CoSD Contract No. 568996
Service Level 46 – Server Software Update
Revision
Peraton/CoSD – 135



Service Level ID	Framework	Service Level	Weighting
		46-5 – Server Software Update - Application Patching for Production PAIDs	1.5%
48	Applications	Project Management Plan Rework	2%

4. Schedule 4.8 Service Levels, Section 10.11 for Server Software Update is hereby amended as per Attachment 1 to this PRR effective March 1, 2024.


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.


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

JOHN M. PELLEGRINO, Director
 Department of Purchasing and Contracting

By: 
 Allen Hunsberger (Mar 1, 2024 15:14 PST)
 Name: Allen Hunsberger
 Title: Assistant Director, Purchasing and Contracting
 Date: Mar 1, 2024

PERATON ENTERPRISE SOLUTIONS LLC

By: 
 Name: Max Pinna
 Title: Contracts Manager
 Email: max.pinna@peraton.com
 Date: Mar 1, 2024

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

Adobe Acrobat Sign Transaction Number: CBJCHBCAABAAacRAv23JuAY2mszy77jbP8r0uESeyhtr

Service Level Service Level ID	Middleware Vulnerability Remediation for Production PAIDs 46-4		
Definition	Remediation of ‘critical’ and ‘high’ vulnerabilities found in middleware software that support production applications.		
Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to implement	<p>Within the rolling 60-day Remediation Cycle (RC), starting on the first day of month and last day of following month (generally 60 days). SL report and exceptions report shall be delivered on the 14th of the month immediately following completion of the RC.</p> <p>Example: If RC #1 period is June 1st through July 31st with reporting due August, then RC #2 period is July 1st through August 31st with reporting due September and so on.</p> <p>Example timeline:</p> <ul style="list-style-type: none"> • Vulnerability scan execution – June 1st • RC #1 period start – June 1st • Vulnerability scan execution – July 1st • RC #2 period start – July 1st • RC #1 period end – July 31st • Vulnerability scan execution – August 1st • RC #3 period start – August 1st • Delivery of report for cycle #1 – August 14th • RC #2 period end – August 31st • Vulnerability scan execution – September 1st • Delivery of report for cycle #2 – September 14th • RC #3 period end – September 30th • Vulnerability scan execution – October 1st • Delivery of report for cycle #3 – October 16th <p>Acceptable exceptions are limited to:</p> <ul style="list-style-type: none"> • Preventing disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April); Employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze; etc.). • Current application version not certified for update of middleware. • Significant upgrade project in progress for PAID will be impacted. <p>Vulnerability remediation shall be applied to development, test, and production environments.</p> <p>Vulnerabilities are identified in the vulnerability scan data provided by the ITO Security team. Though scanning is done more often, the scan data used for this SL will be</p>	80%	90%

	from the scans executed on the 1 st of the month of the appropriate remediation period months.		
Formula	<p>Quantity of in-scope “critical” and “high” middleware vulnerabilities (as identified in the vulnerability scan data) remediated during the RC divided by Quantity of in-scope “critical” and “high” middleware vulnerabilities (as identified in the vulnerability scan data) at the beginning of the RC.</p> <p>“In-scope” quantity excludes acceptable exceptions.</p> <p>“Remediated during the RC” is calculated by comparing the in-scope vulnerability scan results from the end of the current RC to the in-scope vulnerability scan results from the beginning of the current RC. Any in scope vulnerabilities from the beginning of the RC that is no longer evidenced at end of the RC data, is considered “remediated”.</p> <p>For example, for the RC period June 1st through July 31st, formula calculation is as follows:</p> $\frac{\text{(Quantity of “critical” and “high” middleware vulnerabilities remediated during the June RC)}}{\text{(Quantity of in-scope “critical” and “high” middleware vulnerabilities on June 1st scan)}} \text{ divided by } \frac{\text{(Quantity of in-scope “critical” and “high” middleware vulnerabilities on June 1st scan)}}{\text{(Quantity of in-scope “critical” and “high” middleware vulnerabilities on June 1st scan)}}$ <p>Furthermore, for the subsequent RC period July 1st through August 31st, formula calculation is as follows:</p> $\frac{\text{(Quantity of “critical” and “high” middleware vulnerabilities remediated during the July RC)}}{\text{(Quantity of in-scope “critical” and “high” middleware vulnerabilities on July 1st scan)}} \text{ divided by } \frac{\text{(Quantity of in-scope “critical” and “high” middleware vulnerabilities on July 1st scan)}}{\text{(Quantity of in-scope “critical” and “high” middleware vulnerabilities on July 1st scan)}}$		
Measurement Interval	Monthly, based on rolling 60-day RC.		
Reporting Period	<p>Bi-monthly (every two months), based on RC, delivered on the 14th of the month after completion of the RC. The exceptions report will also be delivered on the 14th of the month after completion of the RC. If the 14th of the month is a weekend or holiday, the report will be provided on the next business day.</p> <p>Example: For the RC period June 1st through July 31st, the SL and exceptions reports shall be delivered on August 14th. For the subsequent RC period July 1st through August 31st, the SL and exceptions reports shall be September 14th, and so on.</p>		
Measurement Tool/Source Data	Contractor-provided		

Service Level	Application Vulnerability Remediation for Production PAIDs		
Service Level ID	46-5		
Definition	Remediation of ‘critical’ and ‘high’ vulnerabilities found at the application level for production applications.		
Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to Implement	<p>Within the rolling 60-day Remediation Cycle (RC), starting on the first day of month and last day of following month (generally 60 days). SL report and exceptions report shall be delivered on the 14th of the month immediately following completion of the RC.</p> <p>Example: If RC #1 period is June 1st through July 31st with reporting due August, then RC #2 period is July 1st through August 31st with reporting due September and so on.</p> <p>Example timeline:</p> <ul style="list-style-type: none"> • Vulnerability scan execution – June 1st • RC #1 period start – June 1st • Vulnerability scan execution – July 1st • RC #2 period start – July 1st • RC #1 period end – July 31st • Vulnerability scan execution – August 1st • RC #3 period start – August 1st • Delivery of report for cycle #1 – August 14th • RC #2 period end – August 31st • Vulnerability scan execution – September 1st • Delivery of report for cycle #2 – September 14th • RC #3 period end – September 30th • Vulnerability scan execution – October 1st • Delivery of report for cycle #3 – October 16th <p>Acceptable exceptions are limited to:</p> <ul style="list-style-type: none"> • Preventing disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; Employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze; etc.). • Vulnerability remediation requires an application upgrade. • Significant upgrade project in progress for PAID will be impacted. <p>Vulnerability remediation shall be applied to development, test, and production environments.</p> <p>Vulnerabilities are identified in the vulnerability scan data provided by the ITO Security team. Though scanning is done more often, the scan data used for this service level will be from the scans executed on the 1st of the month of the appropriate remediation period months.</p>	80%	90%

<p>Formula</p>	<p>Quantity of in-scope “critical” and “high” application vulnerabilities (as identified in the vulnerability scan data) remediated during the RC divided by Quantity of in-scope “critical” and “high” application vulnerabilities (as identified in the vulnerability scan data) at the beginning of the RC.</p> <p>“In-scope” quantity excludes acceptable exceptions.</p> <p>“Remediated during the RC” is calculated by comparing the in-scope vulnerability scan results from the end of the current RC to the in-scope vulnerability scan results from the beginning of the current RC. Any in scope vulnerabilities from the beginning of the RC that is no longer evidenced at end of the RC data, is considered “remediated”.</p> <p>For example, for the RC period June 1st through July 31st, formula calculation is as follows:</p> $\frac{\text{(Quantity of “critical” and “high” application vulnerabilities remediated during the June RC)}}{\text{(Quantity of in-scope “critical” and “high” application vulnerabilities on June 1st scan)}} \text{ divided by } \frac{\text{(Quantity of in-scope “critical” and “high” application vulnerabilities on June 1st scan)}}{\text{(Quantity of in-scope “critical” and “high” application vulnerabilities on June 1st scan)}}$ <p>Furthermore, for the subsequent RC period July 1st through August 31st, formula calculation is as follows:</p> $\frac{\text{(Quantity of “critical” and “high” application vulnerabilities remediated during the July RC)}}{\text{(Quantity of in-scope “critical” and “high” application vulnerabilities on July 1st scan)}} \text{ divided by } \frac{\text{(Quantity of in-scope “critical” and “high” application vulnerabilities on July 1st scan)}}{\text{(Quantity of in-scope “critical” and “high” application vulnerabilities on July 1st scan)}}$
<p>Measurement Interval</p>	<p>Monthly, based on rolling 60-day RC.</p>
<p>Reporting Period</p>	<p>Bi-monthly (every two months), based on RC, delivered on the 14th of the month after completion of the RC. The exceptions report will also be delivered on the 14th of the month after completion of the RC. If the 14th of the month is a weekend or holiday, the report will be provided on the next business day.</p> <p>Example: For the RC period June 1st through July 31st, the SL and exceptions reports shall be delivered on August 14th. For the subsequent RC period July 1st through August 31st, the SL and exceptions reports shall be September 14th, and so on.</p>
<p>Measurement Tool/Source Data</p>	<p>Contractor-provided</p>