Problem Resolution Report

CoSD Contract No. 554833
Service Level Updates
Perspecta/CoSD 119

Peraton

Date: January 19, 2023

Summary:

In accordance with the provisions of the IT and Telecommunications Service Agreement No. 554833 (the "Agreement") by and between the County of San Diego ("County") and Perspecta Enterprise Solutions LLC, a Peraton company ("Perspecta" or "Contractor" and hereinafter collectively referred to as the "Parties"), agreement is reached on the Effective Date shown below.

Issue or Problem:

With PRR 113 dated July 25, 2022, the Parties agreed to amend Service Level (SL) 29 – Critical Software Patches to better align the SL measures and performance targets with the County's needs. The Parties also agreed on a 5-month assessment period, August to December 2023, to evaluate the new performance targets. As a result of the SL 29 assessment period and further considerations, the Parties seek further to modify the measures and revise the effective date.

Resolution:

1. Parties agree to extend the assessment period and interim weighting re-assignments established in PRR 113 through January 2023.

2. SL 29-1, 2, and 3 shall become effective February 2023 (with reporting in March) and shall have a combined Weighting Factor of 3%. The Parties agree that should any one of the three SLs miss its respective performance target, the entire SL fails.

3. The interim Weighting Factor assignments established in PRR 113 shall be extended through January 31, 2023. Effective February 2023, the Weighting Factor as per table below shall apply:

SL No.	Description	Weighting Factor February 2023
29	Critical Software Patches	3%
42	Data Restore	1%
32	OIC Additions, Updates and Removals	3%
34	Transaction Response Time - Data Center	3%

4. Section 8.1 - Critical Software Patches of Schedule 4.8, Service Levels, is hereby amended as per Attachment 1 to this PRR.

5. Section 5 - Service Level Summarization and Weighting factors of Schedule 4.8, Service Levels is amended as follows:

Problem Resolution Report

CoSD Contract No. 554833
Service Level Updates
Perspecta/CoSD 119

Service Level Weighting Table			
Service Level ID	Framework	Service Level	Weighting
29-1	End-User	Operating System (OS) I Microsoft Office/Adobe patches involving technical issues and security vulnerabilities	3%
29-2	End-User	Operating System (OS) and Core Software patching for Zero Day Vulnerabilities and any patches ranked as critical by the Contractor security team	
29-3	End-User	Core Software patching that can be distributed via MECM involving technical issues and security vulnerabilities	
32	End-User	OIC Additions and Approvals	3%
34	Network	Transaction Response Time – Data Center	3%
42	Data Center	Data Restore	1%

****

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

By: _____

Name: John M. Pellegrino

Title: Director, Department of Purchasing and Contracting

Effective Date: 1/20/2023

PERSPECTA ENTERPRISE SOLUTIONS LLC

By: _____

Name: Max Pinna

Title: Contracts Manager

Date: January 19, 2023

8.1. CRITICAL SOFTWARE PATCHES

Service Level	Operating System (OS) / Microsoft Office patches involving technical issues and security vulnerabilities		
Service Level ID	29-1		
Definition	Implementation of OS patches and updates for desktop computing assets		
Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to Implement	Measured from the approved mandatory installation deadline which must occur within the timeline respective to the update/patch highest severity rating, per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If the highest severity rating is high, the patch must be deployed within 30 days of the patch release date. If the patch/update is made available on November 1st, the approved mandatory installation must commence before December 1st. If the approved mandatory installation deadline is November 15th, the SLA must be met by December 15th.	93% all PCs	96.5% all PCs
Formula	Qty of workstations patched/updated over patch cycle period ÷ (Qty of workstations in the environment - Qty of Unknown workstations - Qty of Exempt workstations) Unknown workstations are those that have not connected to the County network for an extended period (at least 90 days) and have not accepted the deployment. Exempt workstations are those that have been approved and documented as exempt. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).		
Measurement Interval	Monthly based on Patch Cycle, not on the calendar month.		
Reporting Period	Monthly based on Patch Cycle Initial Report - delivered 7 days prior to completion of the Patch Cycle period Final Report - delivered within 72 hours after Patch Cycle period		
Measurement Tool/Source Data	Contractor-provided		

Service Level	Operating System (OS) and Core Software patching for Critical and Zero Day Vulnerabilities
Service Level ID	29-2
Definition	Implementation of Core Software and OS patches and updates specifically identified as Critical or Zero Day Vulnerabilities. Core Software is defined in Schedule 5, Report 64.

Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to Implement	Measured from the approved mandatory installation deadline which must occur within 15 calendar days as defined per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If the severity rating is Critical, the patch must be deployed within 15 days. If the patch/update is made available on November 1st, the approved mandatory installation must commence before November 15th. If the approved mandatory installation deadline is November 5th, the SLA must be met by November 20th.	93% all PCs	96.5% all PCs
Formula	Qty of workstations patched/updated over patch cycle period ÷ (Qty of workstations in the environment - Qty of Unknown workstations - Qty of Exempt workstations). Unknown workstations (at least 90 days) are those that have not connected to the County network for an extended period and have not accepted the deployment. Exempt workstations are those that have been approved and documented as exempt. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).		
Measurement Interval	As needed based on Critical and Zero Day Vulnerabilities produced with vendor remedy.		
Reporting Period	Initial Report - delivered on day 9 from patch availability from the vendor Final Report - delivered within 72 hours after Patch Cycle period		
Measurement Tool/Source Data	Contractor-provided		

Service Level	Core Software patching involving technical issues and security vulnerabilities		
Service Level ID	29-3		
Definition	Implementation of Core Software patches for desktop computing assets. Core Software is defined in Schedule 5, Report 64.		
Service Measure	Performance Target	SL Performance (%)	SL Earnback
Time to Implement	Measured from the approved mandatory installation deadline which must occur within the timeline respective to the update/patch highest severity rating, per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If the highest severity rating is high, the patch must be deployed within 30 days of the patch release date. If the patch/update is made available on November 1st, the approved	93% all PCs	96.5% all PCs

	mandatory installation must commence before December 1st. If the approved mandatory installation deadline is November 15th, the SLA must be met by December 15th.		
Formula	(Qty of workstations patched/updated over patch cycle period + Qty of in progress workstations patched/updated over patch cycle period) ÷ (Qty of workstations in the environment – Qty of Unknown workstations – Qty of Exempt workstations). In Progress workstations are those that have received the deployment, but the user has not taken the necessary action for the install to complete. Unknown workstations are those that have not connected to the County network for an extended period (at least 90 days) and have not accepted the deployment. Exempt workstations are those that have been approved and documented as exempt. Acceptable Exceptions are limited to prevent disruption of critical business functions (i.e., TTC Property Tax collection periods November-December and March – April; employee benefit enrollment in October; ROV election blackout periods; fiscal year end processing; calendar year-end freeze).		
Measurement Interval	Monthly based on Patch Cycle, not on the calendar month.		
Reporting Period	As Core Patches are Released. Initial Report - delivered 7 days prior to completion of the Patch Cycle period Final Report - delivered within 72 hours after Patch Cycle period		
Measurement Tool/Source Data	Contractor-provided		