Problem Resolution Report

CoSD Contract No. 554833
Service Level Updates
Perspecta/CoSD 113

Peraton

Date: July 25, 2022

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:

The Parties seek to modify the service measurements and/or weights for the following Service Levels:
1. Service Level 29 – Critical Software Patches
2. Service Level 28 – First Call Resolution
3. Service Level 54 – First Call Resolution – 2nd Generation
4. Service Level 42 – Data Restore
5. Service Level 32 – OIC Additions, Updates and Removals
6. Service Level 34 – Transactions Response Time – Data Center

Resolution:

1. The Parties agree to replace the current SL 29 with three new SLs to measure the patching activities for desktop computing assets:

   29-1 – Operating System (OS) / Microsoft Office patches involving technical issues and security vulnerabilities, with an SL Performance Target of 98% for Desktops and 90% for Laptops and Tablets;

   29-2 – Operating System (OS) and Core Software patching for Critical and Zero Day Vulnerabilities, with an SL Performance Target of 98% for Desktops and 90% for Laptops and Tablets; and

   29-3 – Core Software patching involving technical issues and security vulnerabilities, with an SL Performance Target of 98% for Desktops and 90% for Laptops and Tablets.

   SL 29-1, 2 and 3 shall become effective in August 2022 (with reporting in September); however, the Parties agree on a 5-month assessment period, from August through December 2022, to evaluate the Performance Target percentages.

   During the assessment period, SL 29-1, 2 and 3 will be zero weighted and the 3% from SL 29 will be re-assigned as per table below:

SL No.	Description	Current SL Weight (%)	Interim SL Weight (%)
29	Critical Software Patches	3%	0%
42	Data Restore	1%	2%

SL No.	Description	Current SL Weight (%)	Interim SL Weight (%)
32	OIC Additions, Updates and Removals	3%	4%
34	Transaction Response Time – Data Center	3%	4%

The Parties agree that effective January 2023, the weighting percentages for SL 29-1, 2 and 3 will be 3%. Should any one of the SLs miss its respective performance target, the entire SL fails. However, the Parties reserve the right to further mutually revise the SL 29 weighting during the 5-month assessment period.

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

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

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
29-1	End-User	Operating System (OS) / Microsoft Office patches involving technical issues and security vulnerabilities	
29-2	End-User	Operating System (OS) and Core Software patching for Critical and Zero Day Vulnerabilities	0%
29-3	End-User	Core Software patching involving technical issues and security vulnerabilities	
32	End-User	OIC Additions and Removals	4%
34	Network	Transaction Response Time – Internet/Intranet Availability	4%
42	Data Center	Transaction Response Time – Data Center	2%

b. Effective January 2023, the following SLs are updated:

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
29-1	End-User	Operating System (OS) / Microsoft Office patches involving technical issues and security vulnerabilities	3%
29-2	End-User	Operating System (OS) and Core Software patching for Critical and Zero Day Vulnerabilities	

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
29-3	End-User	Core Software patching involving technical issues and security vulnerabilities	
32	End-User	OIC Additions and Removals	3%
34	Network	Transaction Response Time – Internet/Intranet Availability	3%
42	Data Center	Transaction Response Time – Data Center	1%

4. The Parties agree to replace SL 28 – First Call Resolution with SL 54 – First Call Resolution 2nd Generation effective December 2022. Accordingly, the weighting for SL28 is moved to SL54.

5. Section 5, Service Level Summarization and Weighting Factors, of Schedule 4.8, Service Levels, is amended with updates to the following SLs effective December 2022:

Service Level Weighting Table			
Service Level ID	**Framework**	**Service Level**	**Weighting**
28	Service Desk	First Call Resolution	0%
54	Service Desk	First Call Resolution 2nd Generation	3%

****

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

Date: 9/11/2022

PERSPECTA ENTERPRISE SOLUTIONS LLC

By: _____

Name: Max Pinna

Title: Contracts Manager

Date: July 25, 2022

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	Within the Patch Cycle period as measured from one business day after the patch(es) and/or update(s) is made available from the vendor within the current month, through the period as defined by the update/patch highest severity rating per the most recently approved Security Patch Management Procedure (XF.006.006). Example: If vendor makes a patch available on Monday, June 20, and the Security Patch Management Procedure categories the patch as high, the patch cycle period is June 21 – July 21.	98% Desktops 90% Laptops & Tablets	99% Desktops 95% Laptops & Tables
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	Within the Patch Cycle period as measured from one business day after the patch and/or update is	98% Desktops	99% Desktops

	made available from the vendor, up to 15 calendar days as defined per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If vendor makes a patch available on Monday, June 20, and the Security Patch Management Procedure categories the patch as critical, the patch cycle period is June 21 – July 11.	90% Laptops & Tablets	95% Laptops & Tablets
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	Within the Patch Cycle period as measured from one business day after patches and/or updates are made available within the current month, through the period as defined by the update's highest severity rating per the most recent approved Security Patch Management Procedure (XF.006.006). Example: If vendor makes a patch available on Monday, June 20, and the Security Patch Management Procedure categories the patch as high, the patch cycle period is June 21 – July 21.	98% Desktops 90% Laptops & Tablets	99% Desktops 95% Laptops & Tablets

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