Problem Resolution Report

CoSD Contract No. 568996
Privileged Access Management
Peraton/CoSD – 153

Date: July 3, 2025
Title: Privileged Access Management
PRR Number: 153

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:

The Parties wish to add the Privileged Access Management (PAM) services to the Agreement.

PAM is a cybersecurity strategy that focuses on controlling and managing elevated access and permissions for identities, users, accounts, processes, and systems within the County IT environment. This solution will help the County to minimize the attack surface and prevent or mitigate damage from both external attacks and insider threats by right-sizing privileged access controls.

Resolution:

1. Schedule 4.3 Operational Services, Section 2.2. High Level Requirements is amended by adding Sub-section 2.2.10 as follows:

   2.2.10 Contractor shall implement Privileged Access Management (PAM), which exerts control over the elevated ("privileged") access and permissions for accessing the County IT environment.

2. Schedule 4.3 Operational Services, Section 2.18.3 - Roles & Responsibilities, is amended as per Attachment 1 to this PRR.

3. Schedule 16-1 Fees, Section 8, Cross Functional Services is amended by adding sub-section 8.8 as follows:

   8.8 Security Management Services

   As part of Security Management Services, Contractor shall administer and manage Privileged Access Management (PAM) for the County to meet the requirements described in Schedule 4.3, Cross Functional section 2.2.10 and 2.18.3 Roles and Responsibilities. Enterprise license for PAM will be charged separately.

4. This PRR shall be effective the day following the completion of the PAM implementation project.

********** **********

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implemented in accordance with the terms of the Agreement, at which time this Problem Resolution Report shall be deemed superseded and shall be null and void.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

ALLEN R. HUNSBERGER, Director
Department of Purchasing and Contracting

By: Brenda G. Miller
Name: Brenda Miller
Title: Assistant Director
Date: Jul 23, 2025

PERATON ENTERPRISE SOLUTIONS LLC

By:
Name: Max Pinna
Title: Contracts Manager
Email: max.pinna@peraton.com
Date: Jul 23, 2025

By electronically signing this document, all parties accept the use of electronic signatures.
Adobe Acrobat Sign Transaction Number: CBJCHBCAABAA68TGDQvsX6Z_jaCkbp4RW4xQN6ec2Fe-

2.18.3 Roles and Responsibilities

The following table identifies the Plan, Build and Operate roles and responsibilities associated with Identity Access Management Services.

Identity Access Management Services Roles and Responsibilities		
Plan Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit recommended processes for Identity Access Management authentication and authorization.	X	
2. Review and approve processes for Identity Access Management authentication and authorization.		X
3. Produce and submit escalation procedures for quick termination.	X	
4. Review and approve escalation procedures for quick termination.		X
5. Produce and submit End-User Identity Access Management architecture.	X	
6. Establish and manage process to support temporary access.	X	
7. Review and approve End-User Identity Access Management architecture.		X
8. Produce and submit annual End-User account consolidation plan.	X	
9. Review and approve annual End-User account consolidation plan.		X
10. Produce and submit the format for a report detailing all County End-User accounts and End-User data permissions.	X	
11. Review and approve the format for a report detailing all County End-User accounts and End-User data permissions.		X
12. Develop a service ordering process that clearly defines how to order change or delete services.	X	
13. Define logging and archiving policies and requirements.		X
14. Produce and submit recommended processes for Privileged Access Management.	X	
15. Review and approve processes for Privileged Access Management.		X
Build Roles and Responsibilities	**Contractor**	**County**

Identity Access Management Services Roles and Responsibilities		
16. Implement systems to centrally manage and maintain Account Management data and activities.	X	
17. Implement approved processes for Identity, Access and Account Management authentication and authorization.	X	
18. Implement reports detailing all County End-User accounts and End-User data permissions.	X	
19. Implement End-User account consolidation plan.	X	
20. Analyze account management architecture and the access control systems of the County's business applications, and develop and implement an End-User Account Consolidation Plan and End-User Identity, Access and Account Management architecture that provides a platform for account synchronization across the enterprise and across disparate systems.	X	
21. Implement End-User Account Management architecture.	X	
22. Implement escalation procedures for quick termination.	X	
23. Provide logging and archiving specifications/design.	X	
24. Approve logging and archiving specification/design.		X
25. Implement and maintain Privileged Access Management to centrally manage privileged accounts.	X	
26. Implement approved processes for Privileged Access Management.	X	
Operate Roles and Responsibilities	**Contractor**	**County**
27. Centrally maintain End-User accounts.	X	
28. Perform End-User account maintenance to include account creation, deletion or modification.	X	
29. Perform End-User account password resets.	X	
30. Perform End-User authorized data permission requests.	X	
31. Facilitate the receipt and tracking of requests for End-User account activation, changes and terminations.	X	
32. Facilitate the creation, change and deletion of End-User accounts.	X	
33. Coordinate as necessary with other specialized areas to manage End-User accounts.	X	

Identity Access Management Services Roles and Responsibilities		
34. Maintain Access Control Lists (ACL) in accordance with policies.	X	
35. Provide report detailing all County End-User accounts and End-User data permissions on a monthly basis.	X	
36. Provide, update and maintain a reviewable record of security modifications and produce reports and notifications of End-User access modifications, transfers, and terminations.	X	
37. Provide support, including break-fix, for all Identity, Access and Account Management Services.	X	
38. On an annual basis, update the End-User Account Consolidation Plan to reflect progress toward reduction of User IDs and credentials, and to make recommendations for implementation of new technologies within the Identity, Access and Account Management architecture.	X	
39. Support and maintain Identity, Access and Account Management technology solution for infrastructure.	X	
40. Perform engineering, configuration and ongoing management of Identity, Access and Account Management technology solution.	X	
41. Log and archive User/account activity according to approved logging and archiving specification/design.	X	
42. Periodically review production system access logs and activities to identify malicious or abnormal behavior in accordance with established County policies and standards.	X	
43. Periodically review all County account IDs to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established County policies and standards.		X
44. Periodically review all privileged User accounts to ensure the accounts are valid/required, removing inactive and unneeded accounts in accordance with established County policies and standards.	X	
45. Periodically review End-User accounts to ensure each User has appropriate minimal permissions required to perform their job function in accordance with established County policies and standards.	X	

Identity Access Management Services Roles and Responsibilities		
46. Periodically review privileged User accounts to ensure each User has appropriate minimal permissions required to perform their job function in accordance with established County policies and standards.	X	
47. Provide annual report detailing all privileged accounts, as part of the annual renewal of Privileged Access Management subscription.	X	