



**Problem Resolution Report**  
**CoSD Contract No. 568996**  
**Information Security Engineer Labor**  
**Category**  
**Peraton/CoSD – 140**



**Date:** July 1, 2024  
**Title:** Information Security Engineer Labor Category  
**PRR Number:** 140

**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:**

1. The Parties seek to add a new Information Security Engineer Labor Category to the Agreement to address the time and materials (T&M) that Security services provided by Contractor on new projects.

**Resolution:**

1. A new Information Security Engineer Labor Category Resource Unit (RU) is added to the Agreement, with a corresponding hourly RU Fee of \$175.00.
2. Exhibit 16.1-4 – Labor Categories is amended by adding Section 2.29 – Information Security Engineer labor category, as per Attachment 1 to this PRR add the Information Security Engineer labor category, as per Attachment 1 to this PRR.
3. Exhibit 16.1-6 is amended to add the Information Security Engineer RU, as per Attachments 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implemented in accordance with the terms of the Agreement, at which time this Problem Resolution Report shall be deemed superseded and shall be null and void.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.

**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

# Problem Resolution Report

CoSD Contract No. 568996


Information Security Engineer Labor  
Category

Peraton/CoSD – 140



## COUNTY OF SAN DIEGO

JOHN M. PELLEGRINO, Director  
Department of Purchasing and Contracting

By:   
[Allen Hunsberger \(Jul 9, 2024 13:56 PDT\)](#)

Name: Allen Hunsberger  
Title: Assistant Director, Purchasing and Contracting  
Date: Jul 9, 2024

## PERATON ENTERPRISE SOLUTIONS LLC

By: 

Name: Max Pinna  
Title: Contracts Manager  
Email: max.pinna@peraton.com  
Date: Jul 8, 2024

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

Adobe Acrobat Sign Transaction Number: CBJCHBCAABAAF7zXehrjEJ-09\_sVqLzlvXz9kt9oltw7

## 2.29 Information Security Engineer

The Security Engineer is responsible for solution design review, implementation activities, application and infrastructure assessment, compliance enforcement, and identity governance management of internally developed and third-party integrated applications. This includes activities such as vendor assessments, solution assessments, risk assessments, privacy impact assessments, architectural reviews, application/code reviews, infrastructure reviews, compliance reviews and enforcement, role-based identity and access provisioning, research, requirements development, vendor ranking, and assessment. The Information Security Engineer works with various Frameworks and Framework Components such as Contract Management Services, Asset Management, Applications Development, Architecture Development, and Maintenance and Operations. The Information Security Engineer labor category may only be utilized for the performance of services that Contractor is not already required to perform under the Agreement.

### **Knowledge, Skills and Abilities**

Knowledge of:

- Current technology and trends in the profession
- County business and functions

Skills and Abilities:

- Participation in vendor review, assessment, contracts, and onboarding activities
- Participation in solution development, review, assessment, and onboarding activities
- Perform security audit (controls tests) activities
- Perform security risk assessments of potential solutions or vendors
- Perform security risk assessments of existing solutions or vendors
- Perform penetration testing activities
- Perform solution or vendor regulatory and standards compliance assessments
- Perform solution vulnerability scanning assessments
- Perform solution threat modeling assessments
- Perform secure coding assessments
- Perform application integration of single sign-on activities
- Perform implementation of role-based access provisioning
- Perform role-based and least privilege access assessments
- Design, build, review, and implement infrastructure and application security audit logging changes

PRR 140 – Information Security Engineer – Attachment 1  
Exhibit 16.1-4 – Labor Categories

- Perform CIS benchmark hardening activities
- Perform Enterprise environment baseline hardening activities (implementation of guardrails, security controls, policies) (e.g. AWS cloud)
- Design, build, review and implement Active Directory Schema, User Object, Device Object, and Group Policy changes
- Design, build, review, and implement enterprise Certificate/PKI service changes
- Design, build, review and implement Akamai WAF, BOT, Site Shield, API web property security configuration changes
- Design, build, review, implement, and administer Palo Alto Prisma CASB solution and policies
- Design, build, review, and implement secure email gateway/mail flow architecture changes
- Design, build, review, and implement automation scripts
- Define regulatory controls and changes
- Define solution hardening standards
- Define secure application development standards

**Education and/or Experience:**

Education, training, and/or experience that demonstrate possession of the knowledge, skills and abilities listed above. Examples of qualifying education/experience:

1. Bachelor's or equivalent university degree and a minimum seven (7) years of experience working in information security architecture, information security governance, risk and compliance, information security threat and vulnerability management, and/or identity governance and administration; **OR**
2. Information Assurance Management (IAM) **or** Information Assurance Technical (IAT) certifications level 3 plus 5 years' experience.
3. IAM **or** IAT certification level 2 plus 7 years' experience.
4. IAM **or** IAT certification level 1 plus 9 years' experience.

