Cybersecurity Architect Performance Profile

Opportunity Overview

This full-time remote opportunity with Technology Transformation Services (TTS) Delivery Office within the Technology Operations Division. TTS is a part of the U.S. General Services Administration (GSA) under the Federal Acquisition Services (FAS) Organization. TTS applies modern methodologies and technologies to improve the public's experience with government by helping agencies make their services more accessible, efficient, and effective.

The TTS Technology Operations Division oversees, manages and coordinates everything technology-related across TTS, and anything technology-related that will affect TTS from the outside, particularly security, compliance, infrastructure, and policy.

Position Summary (Public)

As the Cybersecurity Architect, you will review TTS security measures, recommend enhancements, identify areas of weakness, and respond promptly to possible security breaches. You will be responsible for preparing recommendations to improve TTS' security posture and optimize the delivery of secure services. You will act as the primary liaison between TTS and GSA IT Security to coordinate with system owners, common control providers, and/or system security officers on the allocation of security controls as system-specific, hybrid, or common controls.

Key Objectives

1. **Implement organizational security architecture best practices**
    - Plans, develops, and implements policies & procedures consistent with CISO objectives as they pertain to cybersecurity risk management in the IT environment
    - Plays a key role in formulating, developing, and implementing strategies, standards, and guidelines for TTS programs and functions in support of the authority to operate (ATO) process
    - Stays abreast of current and emerging security and privacy regulations that may impact systems and aids in the development of recommendations and roadmaps for impacted TTS systems
    - Develop internal processes and metrics for measurement of overall cybersecurity readiness and then communicates status to leadership and other stakeholders
    - Analyzes TTS systems and platforms against current cyber threats, regulations and policies, identifies gaps, and then develops recommendations for future TTS prioritization and investment
    - Works closely with the CISO on the execution of security relevant portions of the agency's Information Assurance Program including ensuring systems are properly authorized for operation
    - Ensures sufficient technological and administrative measures are implemented
        - Make sure the security of TTS data systems, processes, and facilities
        - Confirm the use of technology sustains and does not erode security protections relating to the use, collection, and disclosure of mission critical information

2. **Provide subject matter expertise in secure systems architecture on behalf of TTS**
    - Oversee and provide guidance on the implementation of cybersecurity requirements during all phases of program and/or system life-cycle
    - Develop a complete understanding of TTS systems and supporting platforms to include Cloud.gov, Login.gov, and supporting software as a service (SaaS) products

- Ensure acquired or developed system(s) and architecture(s) are consistent with GSA's cybersecurity architecture guidelines
    - Give guidance on secure network, software, and systems development practices
    - Develops and interprets guidance for TTS compliance procedures and operations
    - Assists system teams with secure standardized architectural implementations to increase speed of delivery
    - Provides guidance and assistance to system teams on the integration with standardized security tooling in order to meet security control requirements
- Identifies opportunities for consolidation and normalization of security capabilities and architecture across system teams
- Assists system teams post security incidents to identify and make recommendations for system, platform, and organizational improvements
- Document and address GSA's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle
    - Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents

3. **Provide project management support for Technology Operations**
    - Lead a high performing contract staff in support of TTS-wide information security activities
    - Act as a liaison between TTS and GSA IT shared service providers in order to increase awareness and use of enterprise services
    - Develops plans, makes recommendations, and assists system teams with the automation of security compliance activities

Desired Skills

- Experience with the design, implementation, documentation and operations of securely architected systems, including:
    - Designing and implementing multi-factor authentication for information systems
    - Performing threat modeling; analyzing system, process, and business logic for vulnerabilities, beyond traditional scanning
    - Encryption of data in transit and at rest utilizing FIPS 140-2 or 140-3 validated encryption including the use of hardware security modules (HSM)
    - Developing justifications, compensating controls, and requesting exceptions when a security control or vulnerability cannot be pragmatically and effectively met or remediated
    - Secure leveraging of FedRAMP Software, Platform, and Infrastructure cloud services based on outlined customer responsibilities
- Experience with the following technologies:
    - Git version control
    - Containerization technologies
    - Scripting in a UNIX and/or Windows environment
    - Infrastructure as Code (Terraform, Ansible, Chef, and Puppet)
    - Networking such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services