Security Engineer 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 Security Engineer within the Technology Operations Division, you will analyze, document, and develop strategies to mitigate security and privacy risks posed by today's rapidly changing information technology. You must have the knowledge and skills sets necessary to analyze complex systems and processes and explain risks to both technical and business audiences. Critical and innovative thinking, strong writing, and adaptability are a must.

Key Objectives

1. **Provide expert technical guidance, interpretation, and implementation oversight of applicable cybersecurity policies, processes, and practices to ensure continued availability of TTS information systems.**
   - Advise the Tech Operations Director on the latest IT security and privacy cloud technologies to aid in decision making
   - Develop a complete understanding of TTS systems and supporting platforms to include Cloud.gov, Login.gov, and supporting software as a service (SaaS) products
   - Assists system teams post security incidents to identify and make recommendations for system, platform, and organizational improvements
   - Develops threat models and security requirements for Application Programming Interfaces (API)
   - Review IT security programs to assess overall compliance with cybersecurity plans and policies, as well as their alignment with business requirements
   - Assesses security risks and vulnerabilities; builds, tests, and recommends cloud security solutions; and manages cloud environments in accordance with GSA approved cybersecurity security guidelines
   - Collaborate with other engineers to design and develop specific applications/ methodology.

2. **Ensure TTS SaaS products obtain the appropriate authorization to operate (ATO)**
   - Serve as the liaison between TTS and GSA IT Security for all IT security related activities
   - Demonstrate expertise in security industry standards (e.g., NIST 800 series) and best practices
   - Lead efforts in accordance with the Federal Information Security Management Act (FISMA) to ensure the protection of TTS IT assets.
     - Participates in conducting and/or managing independent evaluations and compliance reviews of TTS IT systems in accordance with FISMA

- Write the security documentation for the authorization package
    - System Security Plan, Digital Identity Acceptance Statement, Privacy Threshold Assessment, Privacy Impact Assessment, etc.
- Experience with IT security assessment and authorization processes, security risk assessments, implementation of IT security controls and countermeasures and associated technologies
- Develop, maintain, and facilitate the appropriate closure of plan of action & milestone (POA&M) findings and any related remediation activities

3. **Perform operations rotation duties**
    - Assist the TTS workforce with non-standard IT requests
        - Automate the process using tools such as ServiceNow
            - Develop the business and technical requirements
            - Create standard operating procedure (SOP) to explain the process
    - Conduct user account management for IaaS/PaaS/SaaS products
        - Create AWS sandbox and jump accounts
        - Run terraform linting and security scans
        - Perform GitHub administrative functions (e.g. pull requests)

4. **Provide project management support for Technology Operations**
    - Lead projects to design, acquire, and implement major prototype and developmental systems or to make extensive modifications and upgrades to existing systems
    - Develops plans, makes recommendations, and assists system teams with the automation of security compliance activities
    - Promote awareness of security issues among management and ensure sound security principles are reflected in organizations visions and goals

Desired Skills

- Ability to handle multiple priorities and communicate expectations up/down the chain
- Knowledge of software product delivery in a federal DevOps environment
- Apply advanced theories, concepts, principles and processes of engineering and support cybersecurity efforts through research, identifying, and recommending solutions to cyber threats
- Experience with the design, implementation, documentation and operations of securely architected systems, including:
    - Designing and implementing multi-factor authentication for information systems.
    - Secure leveraging of FedRAMP Software, Platform, and Infrastructure cloud services based on outlined customer responsibilities.
- Experience with the following technologies:
    - Git version control
    - Web Application Security
    - Amazon Web Services (AWS)
    - Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
    - Security information and event management (SIEM)
        - Endpoint Monitoring/Forensics
        - Log Analysis/Monitoring/Alerting