MANAGER OF CYBER SECURITY

JC: 000071
PB: 10
FLSA: Exempt

BU: 92 (NR)
Created: September 2013
Revised: June 2019

*Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are **not** intended to reflect all duties performed within the job.*

DEFINITION

Under general direction, manages and oversees the Cyber Security team in designing, implementing, and maintaining the District's Unified Cyber Security Program. Responsibilities include identifying institutional security vulnerabilities, designing enterprise remediation solutions, designing complex algorithms to monitor both machine and human behavior, and identifying core metrics to measure the effectiveness of security solutions; performs related duties as required.

CLASS CHARACTERISTICS

This is a full-scope managerial level classification responsible, through subordinate professionals, for managing and executing Information Security project work plans including drafting, validating, and approving all cyber security policies, procedures, standards, and guidelines and makes recommendations to executive management. Positions at this level are accountable for accomplishing division goals and objectives, following operating procedures and policies, technical decision making, budget administration and personnel management. This classification is distinguished from the Director of Information Technology in the latter is responsible for the operations and activities of the District's Cyber Security Division of the Office of the Chief Information Officer Department.

REPORTS TO

Directory of Information Technology or designee.

EXAMPLES OF DUTIES – *Duties may include, but are not limited to, the following:*

1. Manages and oversees the designs, implementation and maintains District's Unified Cyber Security Program including the validation and approval of all Cyber Security policies, investigations, and procedures.

2. Identifies institutional Cyber Security vulnerabilities and designs enterprise remediation solutions; Designs complex computer algorithms used to monitor both machine and human behavior.

3. Performs front line operations for police networks.

4. Develops and negotiates vendor contracts and manages vendors relationships.

5. Acts as a resource for management in the selection of hardware, software and consulting services related to District Infrastructure.

6. Participates in the Communication Information Office (CIO) leadership team, offering recommendations to the District's Technology as needed; Certifies Cyber Security within the District's Technology Project Approval Process.

7. Identifies core metrics to measure the effectiveness of security solutions; Performs post-mortem forensic cyber investigations after breach.

8. Works with District stakeholders to establish design guidelines and architectural standards for security-related investments.

9. Works with Local, State and Federal officials to coordinate Cyber Defense Initiatives.

10. Performs other duties as assigned.

QUALIFICATIONS

Knowledge of:

- Principles of information security tools, architecture and security control
- Principles and practices of business processes and project management
- Methods of emergency management approaches and procedures
- Cyber Security standards and practices
- Information Systems and Information Security which address organizational structure administration practices, system development and maintenance procedures, system software and hardware controls, security and access controls, computer operations, environmental protection and detection, and backup and recovery procedures
- Information system architecture and security controls, such as firewall and border, router configurations, operating systems configurations, wireless architectures, databases, specialized appliances and information security policies and procedures
- Technologies such as IDS/IPS, vulnerability assessment tools, remote access methodologies, log management tools, firewalls, cryptography and digital certificates
- Programming languages such as Java, C, C++, C#, and .NET
- Industry Standards, eg, ISO 17799/27001, NIST Publications and other Industry Related Security Standards
- Related Federal, State and local laws, codes and regulations pertaining to work and to generally accepted industry and associations standards

Skill/Ability in:

- Developing and writing Cyber Security Policy and Procedures
- Utilizing information security tools such as Nessus, Kismet, Airsnort, NMAP, Ethereal, WebInspect and Nikto
- Performing manual techniques to exploit vulnerabilities in the OWASP top 10; including but not limited to cross-site Scripting, SQL injections, session hi-jacking and buffer overflows to obtain controlled access to target systems

- Performing network traffic forensic analysis, utilizing packet capturing software, to isolate malicious network behavior, inappropriate network use or identification of insecure network protocols
- Analyzing and testing attack and penetration of Internet infrastructure and Web-based applications utilizing manual and automated tools
- Preparing clear and concise reports and documentation. Executing troubleshooting tasks
- Application source code security review
- Establishing and maintaining effective working relationships with those contacted in the course of work
- Developing and writing cyber policies and procedures
- Coordinating with District management, local law enforcement, and federal law enforcement
- Understanding complex Enterprise network and application architecture
- Maintaining life safety network systems for BART train operations and policing
- Managing highly complex and sensitive response scenarios to remediate and restore system failures due to cyber events
- Interpreting and applying Federal, State and local policies, laws and regulations
- Communicating clearly and concisely, both orally and in writing
- Establishing and maintaining effective working relationships with those contacted in the course of work

MINIMUM QUALIFICATIONS

Education:
Bachelor's degree in Information Technology, Computer Science, Information Security or a closely related field from an accredited college or university.

Experience:
Five (5) years of (full-time) professional verifiable experience in Data Center Cyber Security or related experience which must include at least two (2) years of supervisory experience.

Substitution:
Additional professional experience as outlined above may be substituted for the education on a year-for-year basis. A college degree is preferred.

License or Certificate
Professional certifications such as CISSP, CCNA or similar certification preferred.

Other Requirements:
Physical condition necessary to conduct field inspections and testing as assigned.

WORKING CONDITIONS

Environmental Conditions:
Office environment; exposure to computer screens.

Physical Conditions:
May require maintaining physical condition necessary for sitting for prolonged periods of time.

BART EEO-1 Job Group: 3000 – Engineers
Census Code: 1007 – Information Security Analysts
Safety Sensitive: No