Job Description

Please note this job description is not designed to cover or contain a comprehensive listing of activities, duties or responsibilities that are required of the employee for this job.

Job title	Cybersecurity Engineer

GENERAL PURPOSE

Under general direction, serves in a technical expert capacity for the District's cybersecurity and risk assessment program; leads the District's cybersecurity team; assumes responsibility for the development and management of security policies for District infrastructure, communications, and software systems and devices; monitors systems, tests for vulnerability and takes proactive or reactive actions to protect the District's assets; and performs related duties as assigned.

DISTINGUISHING CHARACTERISTICS

This is a professional program-management classification responsible for planning and directing the design, development, implementation and management of a comprehensive cybersecurity program for the District's technology operations. Incumbents are responsible for performing diverse, specialized and complex work involving significant accountability and decision-making by exercising primary responsibility for cybersecurity related operations. Incumbents serve as a professional-level resource for organizational, managerial, and operational analyses and studies, employee will normally require access to highly sensitive and confidential information. Performance of the work requires the use of considerable independence, initiative, and discretion within broad guidelines.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from assigned management personnel. Exercises functional or technical direction over and provides training to lower-level staff.

TYPICAL DUTIES AND RESPONSIBILITIES

The duties listed below are intended only as illustrations of the various types of work that may be performed. The omission of specific statements of duties does not exclude them from the position if the work is similar, related or a logical assignment to this position.

- Plans, directs, and oversees the execution, implementation and ongoing management of the District's Cybersecurity Program; serves in a technical expert capacity for the District's information technology security and risk assessment operations.
- Collaborates with District departments and technology staff in the development and deployment of policies and procedures designed to mitigate the District's exposure to

cybersecurity threats; conducts research to identify best management practices in cybersecurity program management to guide the District in implementing a program which meets their needs.

- Creates secure network architectures which embed security measures designed to ensure the protection of network infrastructure, servers, data storage, communications and enterprise software systems; develops and prepares specifications for group policy and Windows configuration management.
- Leads the work of a team responsible for performing proactive and reactive security related tasks; identifies team member roles and responsibilities, and provides technical guidance on same; ensures team members have sufficient training to perform their security-related roles.
- Monitors systems and networks for security threats or breaches; conducts assessments to test areas of vulnerability; designs and implements solutions which meet the District's security standards.
- Responds to security threats and incidents; takes timely and decisive actions to protect the District's assets; works with the team to determine the scope and magnitude of the incident, systems impacted, containment measures, and immediate solutions; develops and implements short or long proactive security measures for future deterrence.
- Conducts audits and prepares reports on technology assessments for District operations with high impact risks and/or regulatory requirements which mandate specific risk deterrent measures including, but not limited to, financial or environmental impacts; prepares findings and recommendations to enhance security measures for compliance with mandatory regulations and risk reduction directives.
- Develops and implements protocols for response to system threats and intrusions including response times, measures to contain the impact, and disaster recovery procedures.
- Observes and complies with all District and mandated safety rules, regulations, and protocols.
- Performs related duties as assigned.

REQUIRED QUALIFICATIONS

Knowledge of:

- Industry best practices in the design and development of cybersecurity measures for enterprise systems, network infrastructure and software in multiple platforms and operating environments including, but not limited to, cloud and wireless security, remote access, and application containerization/virtualization.
- Industry resources for cybersecurity support, information sharing and communication/notification tools.

- Methods and techniques of evaluating security related technology threats and responding accordingly.
- Methods and techniques of developing security and disaster recovery protocols, processes and procedures.
- Technology threat/intrusion protection systems and devices, and their effectiveness in specific technology areas.
- Encryption technologies and products.
- Methods and techniques of conducting risk assessments for a diverse range of District operations.
- Diagnostic tools and utilities used in proactive and reactive threat detection and response situations, including vulnerability scanning, and penetration testing tools and equipment.
- Principles and practices of leadership.
- Principles and techniques for working with groups and fostering effective team interaction to ensure teamwork is conducted smoothly.
- Change management principles and practices.
- Principles and practices of project management.
- Federal, state, and local laws, codes, and regulations in assigned areas of responsibility.
- District and mandated safety rules, regulations, and protocols.
- Techniques for providing a high level of customer service by effectively dealing with the public, vendors, contractors, and District staff.
- The structure and content of the English language, including the meaning and spelling of words, rules of composition, and grammar.
- Modern equipment and communication tools used for business functions and program, project, and task coordination, including computers and software programs relevant to work performed.

Ability to:

- Use modern, state-of-the-art methods to design and implement critical systems proactive and reactive security measures and protocols.
- Plan, organize and execute cybersecurity related initiatives in order of priority and criticality.
- Monitor security measure effectiveness and recommend changes to optimize system resistance to security threats and breaches.
- Analyze and define user requirements and recommend efficient, secure and cost-effective architectures.
- Prepare concise technical guides, system documentation and specifications for technical staff.
- Audit department operations to identify technology system risks and prepare reports identifying solution measures.
- Ensure solutions and actions taken support the District's cybersecurity goals and

objectives.

- Stay current with best management practices for cybersecurity programs, diagnostic tools, and mitigation measures.
- Conduct comprehensive research on a diverse range of cybersecurity topics.
- Effectively lead the work of project teams to accomplish technology program goals and objectives.
- Conduct analysis and feasibility studies; analyze complex problems, evaluate alternatives, and make sound recommendations.
- Demonstrate several key security practices in access control, application security, network security, security architecture, and security strategy.
- Apply critical thinking techniques for a broad range of situations.
- Prepare clear, concise, and accurate reports and technical documentation.
- Independently organize work, set priorities, meet critical deadlines, and follow-up on assignments.
- Use tact, initiative, prudence, and independent judgment within general policy, procedural, and legal guidelines.
- Effectively use computer systems, software applications relevant to work performed, and modern business equipment to perform a variety of work tasks.
- Communicate clearly and concisely, both orally and in writing, using appropriate English grammar and syntax.
- Establish, maintain, and foster positive and effective working relationships with those contacted in the course of work.

<u>Experience:</u>

Any combination of experience and education that provides the required knowledge and abilities is qualifying, along with the specific licenses/certifications as outlined below:

Required:

- Five (5) years of progressively responsible professional experience in cybersecurity program design, development and management.
- Two (2) years of professional experience in mobile device management and desktop/client deployments.
- Designing, implementing, securing, and managing medium to large Windows Active Directory 2012+ domains utilizing Group Policy and Windows Software/Server Update Services (WSUS).

Desired:

- Firewall management: Fortigate/Palo Alto preferred, Cisco ASA/Firepower acceptable.
- Web application filtering, reverse proxy techniques, and Cloudflare experience a plus. Office365 and Microsoft Azure management experience a plus.

Education:

- Equivalent to a bachelor's degree from an accredited college or university with major coursework in information technology, computer science, cybersecurity, or a closely related field.

Licenses/Certifications:
The most competitive applicants will hold one or more of the following certifications:

- (ISC)2: Certified Information Systems Security Professional(CISSP), Systems Security Certified Practitioner(SSCP), Certified Cloud Security Professional(CCSP)
- GIAC: Defensible Security Architecture (GDSA)/Certified Detection Analyst (GCDA)/Critical Controls Certification (GCCC), Global Industrial Cyber Security Professional(GICSP)/GIAC Response and Industrial Response (GRID)/Critical Infrastructure Protection (GCIP), Forensic Analyst (GCFA)/ Network Forensic Analyst (GNFA)/Cyber Threat Intelligence (GCTI)
- ISACA: Certified Information Systems Auditor(CISA)
- Cisco: Certified Network Professional (CCNP) Routing & Switching or Security, Certified Internetwork Expert (CCIE) Security
- Fortinet: Network Security Expert (NSE) 4
- Microsoft: MCSA: Windows Server 2012/2016, MCSE: Core Infrastructure

Required:
- A valid California driver's license and the ability to maintain insurability under the District's Vehicle Insurance Policy.

PHYSICAL DEMANDS

The physical demands described here are representative of those that must be met by employees to successfully perform the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Must possess mobility to work in a standard office setting and use standard office equipment, including a computer; vision to read printed materials and a computer screen; to operate a motor vehicle and visit various District sites; and hearing and speech to communicate in person and over the telephone. This is primarily a sedentary office classification although standing in work areas and walking between work areas may be required. Finger dexterity is needed to access, enter, and retrieve data using a computer keyboard or calculator and to operate standard office equipment. Positions in this classification occasionally bend, stoop, kneel, reach, push, and pull drawers open and closed to retrieve and file information. Employees must possess the ability to lift, carry, push, and pull materials and objects up to 40 pounds.

WORK ENVIRONMENT

The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this class. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Employees work in an office environment with moderate noise levels, controlled temperature conditions, and no direct exposure to hazardous physical substances. Employees may interact with upset staff and/or public and private representatives in interpreting and enforcing departmental policies and procedures.

This job description has been reviewed and approved by all levels of management in cooperation with the union (if applicable):

Approved by:	
Date adopted:	
Date modified:	
FLSA determination:	*Exempt*

Job Description Acknowledgment

I have received, reviewed, and fully understand the job description for Cybersecurity Engineer. I further understand that I am responsible for the satisfactory execution of the essential functions described therein, under any and all conditions as described.

Employee Name (print): ______________________________ *Date:* ____________

Employee Number: ____

Employee Signature: ____