# Information Security Officer

## DEFINITION

Under general direction from the Information Technology Manager and within the framework of established policies and procedures, plans, organizes, coordinates and implements District-wide cybersecurity compliance activities and operations, to ensure the confidentiality, integrity and availability of information technology systems; serves as an internal consultant on cybersecurity and information privacy; to improve cybersecurity risk management; and performs a variety of professional and technical level tasks relative to assigned area of responsibility

## DISTINGUISHING CHARACTERISTICS

The incumbent in this position directs the District-wide information technology security program while performing the full range of routine to complex and specialized technical activities in cybersecurity and information privacy. Assignments are given in general terms and subject to periodic review while in progress and upon completion by the Information Technology Manager. There is significant latitude for discretion and independent judgment in the selection of work methods to achieve established goals.

This classification is distinguished from the Information Technology Manager, in that the latter is a division manager with overall administrative responsibility for the District's Information Technology program and supervises this classification. It is distinguished from the Senior Information Systems Analyst in that the Security Officer performs the most complex and specialized cybersecurity work and may provide direction to persons in the analyst classifications. It is distinguished from the Information Technology Supervisor in that the Security Officer has full program responsibility for cybersecurity compliance and operations and does not supervise staff involved in more general Information Technology analysis and activities.

## TYPICAL DUTIES

**TYPICAL EXAMPLES OF DUTIES MAY INCLUDE, BUT ARE NOT LIMITED TO THE FOLLOWING:**

- Coordinates the continuous development, implementation, and updates of information security and privacy policies, standards, guidelines, baselines, processes, and procedures in compliance with best practices and local, state, and federal regulations.

- Develop and implement a comprehensive cybersecurity program by researching, identifying, and analyzing existing and potential security threats; develop and manage the frameworks, processes, and tools necessary to properly manage risk and to make risk-based decisions related to Information Technology (IT) and Operational Technology (OT), including but not limited to Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA)activities.

- Implement processes to continuously monitor District software and systems for vulnerabilities; monitor logs and alerts for security events; assist IT and SCADA systems staff in patching and updating District systems on a continuous basis; monitor and assess the success of patching and updating of District systems and infrastructure.

- Lead and participate in complex projects designed to provide for the protection of District information assets; recommend solutions and appropriate technology to meet District needs; design project and resource plans and schedules; develop proposals using cost/benefit

  analysis; evaluate proposed system hardware and software to ensure compatibility with existing systems; coordinate with vendors and contractors.

- Provides functional supervision to District staff involved in cybersecurity projects and activities.

- Proactively identify and mitigate cybersecurity risks and respond to observations identified by third-party auditors/security service providers.

- Review cybersecurity vulnerabilities and conduct penetration testing on a periodic basis.

- Develop periodic reports and dashboards presenting the level of controls, compliance, and current IT and SCADA risk posture.

- Lead, implement, and maintain District-wide training related to cybersecurity.

- Represent information security and privacy function on committees and outside organizations as necessary; coordinate emergency preparedness activities and tabletop exercises related to cybersecurity.

- Assist IT and SCADA Administrators in creating, implementing, and testing emergency and disaster recovery measures that ensure continual operational readiness of District systems.

- Work closely and collaborate with other departments' staff responsible for OT and SCADA systems.

- Serve as the District's central point of contact for information security-related incidents or violations; investigate and document cybersecurity incidents; lead and assist in remediation of cybersecurity incidents and vulnerabilities and make recommendations for improvements.

- Coordinate information security incident response and reporting for events or exploited vulnerabilities, including unauthorized system or network access, denial of service, inappropriate data access, data corruption, and/or collection of private or confidential information.

- Work as a liaison with local, state, and federal authorities requiring information and reports on security incidents to FBI or other law enforcement agencies.

- Participate in budget preparation; prepare cost estimates for budget recommendations; submit justifications for program materials, equipment, supplies, and services

- Stay abreast of new trends and developments in the areas of cybersecurity, networking, server and storage systems, disaster recovery; attend and participate in group meetings.

- Perform other related work as required

## REQUIREMENTS

*Any combination of education and experience that would likely provide the required knowledge, skills, and abilities is qualifying. A typical way to obtain the knowledge, skills, and abilities would be the equivalent of:*

**Education and Experience:**
Possession of a bachelor's degree from an accredited college or university with a major in information systems, computer science, or closely related field **and** five (5) years progressively responsible professional level work experience in information security.

**Additional Requirements:**
- Must possess a valid California driver's license and have a satisfactory driving record.
- Possession of information technology security certifications such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) are highly desirable.

**Knowledge, Skills and Abilities:**
Thorough knowledge of: principles, practices, methods, and techniques used in the network and cyber security systems operation, maintenance, and administration across multiple platforms for both IT and SCADA environments; understanding of information technology and SCADA privacy and security concepts, best practices, applicable laws and standards, and understanding of relevant emerging cybersecurity threats and issues; knowledge of enterprise systems, networking, security appliances such as firewalls, computer operating systems, virtualization platforms, storage area networks and backup and recovery systems; design and implementation of complex information technology architectures; principles and techniques of work and project planning, prioritizing and scheduling applicable to information technology; safe work practices and the ability to identify workplace hazards and/or unsafe conditions and take appropriate action; knowledge of laws and regulations such as HIPAA, PCI; knowledge of IT and SCADA/Industrial Control System (ICS) processes and controls and strong understanding of risk and control frameworks such as (CoBIT, ISO, NIST, ITIL).

Skill and Ability to: plan, coordinate, and monitor complex projects and programs; analyze and solve complex technical problems, evaluate alternatives, make recommendations and take effective actions; understand principles and practices of computer networking and cybersecurity; understand and apply risk based cybersecurity and control frameworks; prepare clear and concise documentation, user procedures, reports of work performed and other written materials; communicate effectively, both orally and in writing including providing technical information in non-technical terms; provide instruction and training to end users; establish and maintain designated documentation and records in an accurate and timely manner; ability to work collaboratively and in a team based environment; establish and maintain effective working relationships with those contacted in the performance of required duties.

**Working Conditions/Physical Requirements:**
The essential functions of the job require on a continuous basis, the ability to sit for extended periods of time in front of a computer screen; intermittently twist to reach equipment or supplies surrounding desk; perform simple grasping and fine manipulation; use telephone, computer keyboard and related equipment on a daily basis; speak and hear in person and on the phone; see sufficiently to perform assignments; periodically drive a vehicle and frequently lift and/or carry objects weighing up to 25 pounds and occasionally up to 55 pounds.

The essential functions of this classification require frequent driving to perform essential job duties which may include attending meetings or doing business at various off-site locations. Alternative forms of transportation are not suitable due to security concerns, logistical challenges, and time constraints.

Revised: 03/2025

Approved: Amy M Reeve
Human Resources/Risk Manager