Department of Toxic Substances Control
Position Duty Statement

Classification Title Information Technology Specialist III	**Department** Department of Toxic Substances Control
Working Title Senior Information Security Engineer	**Office/Unit/Section/Geographic Location** Office of Environmental Information Management/ Enterprise Security Services Unit/Sacramento Headquarters
Position Number 810-250-1415-002	**Effective Date**

General Statement: Primary Domain: Information Security Engineering; Secondary Domain: Systems Engineering, Software Engineering. Under the administrative direction of the Information Technology Manager II of the Enterprise Security Services Unit, the Information Technology Specialist III (ITS III) will serve as the Senior Information Security Engineer. The incumbent will perform Information Technology (IT) support functions that support and continuously improve the Department of Toxic Substances Control's (DTSC) security posture, and will operate independently but within a clear accountability framework. All duties are performed within the framework of the Department's Mission and Vision statements, and in accordance with the Department's Policies and Procedures. Specific duties include, but are not limited to:

A. Specific Activities: Essential (E) / Marginal (M) Functions

25% (E) Security Operations

In a leadership capacity, participates in the security operations planning with the Security Services Manager and the Information Security Officer (ISO). Acts as the Security Operation Center (SOC) Team Lead. Develops documentation, including design diagrams, operating procedures, root cause analysis, reports, troubleshooting and responses for audits and assessments. Performs investigations of potential security incidents and upon request of the ISO. Responds to security requests and tickets, including but not limited to those requiring the Information Security Unit's technical review/approval, TEIR III technical support from the Information Security Services and responding to alerts. Collaborates with the ISO in the development of security standards. Works in partnership with other technical team leads, such as application developers, network engineers and server administrators to ensure required security controls are in place and functioning as expected. Works with technical leads throughout the division to develop baseline configurations. As team lead, mentors other staff in the Security Services Unit and other IT domains. Provides security operations subject matter expertise relating to projects efforts, network security and security operations.

20% (E) Information Security Architecture

Advises, creates, and participates in the design of new system architecture, standards, and methods to support the organization's technology strategies. Collaborates with other technology architects in the design of solutions to advise on security best practices. Performs the lead role in the implementation of security services including continuous monitoring, incident response, network security, threat hunting, etc. Applies knowledge of network security to identify risks relevant to projects and the DTSC network and information assets. Triages findings from security tools, summarizes findings in high-level reports and applies remediation after security governance approval. Deploys tools to help automate and augment security checks. Provides support for technology recovery planning including recovery strategies, risk assessments, training, and Technology Recovery Plan exercises. Works with stakeholders to perform threat modeling/architecture risk analysis on new design proposals. Attends Change Management Board meetings with a focus on network configuration oversight. Provides Information Security Program planning assistance within the realms of network security, forensic investigation, IT architecture, operations, system administration and security compliance.

20% (E) Incident Response

Leads the team in actively responding to security incidents. Analyzes business impact and exposure, based on emerging security threats, vulnerabilities and risks and recommends mitigative solutions. Researches, documents, and develops reusable security defense procedures/playbooks in responding to security incidents. Provides advanced root cause analysis to identify or resolve issues that may cause impact to the DTSC environment. Updates, revises, and provides feedback on Incident Response plans and playbooks on a consistent basis. Performs a leadership role within the DTSC Incident Response Plan. Participates in Incident Response Plan testing.

15% (E) Security Infrastructure Administration

Deploys, administers, operationalizes, and maintains information security systems and appliances. Implements and maintains DTSC's information security solutions. Coordinates systems installation, operations, maintenance, repairs, and upgrades of security appliances and infrastructure. Develops security services unit's standard operating procedures in partnership with team members. Consults with stakeholders to identify business impacts and exposure for IT solutions, based on emerging security threats, vulnerabilities, and risks to recommend solutions.

10% (E) Security Education and Training

Researches and communicates about new cyber security trends, tactics, vendors, and solutions. Promotes innovation by empowering collaborative and secure service between technology and DTSC program. Provides expert knowledge of industry trends and technologies as they relate to specific opportunities where security can enhance value to the business and/or address a specific business needs. Communicates, educates, and reminds staff of new security threats, best practices, and policies, guidelines and standards.

5% (M) Administrative Duties

Responsible for performing administrative duties including, but not limited to: adheres to Department policies, rules, and procedures; submits administrative requests including leave, overtime, travel, and training in a timely and appropriate manner; accurately reports time in the Daily Log system and submits timesheets by the due date.

5% (M) Other related duties as required

Other related duties, as assigned within the classification of this position.

B. Supervision Received

The ITS III reports directly to and receives most assignments from the ITM II. However, direction and assignments may also come from the Chief Information Officer, Chief Technology Officer, ISO, Chief Deputy Director, Director, and other IT Managers. The ITS III may also receive direction on Agency-wide security policies and activities from the Agency Information Officer or Agency Information Security Officer.

C. Supervision Exercised

None.

D. Administrative Responsibilities for Supervisors and Managers

None.

E. Personal Contacts

The ITS III effectively communicates and collaborates with all levels of staff throughout the Department.

F. Actions and Consequences

There are four areas where there could be consequences to OEIM and/or the Department if the job is performed inadequately. They include:

1) Failure to properly direct, detect, report, and mitigate security breaches and intrusions could result in the release of sensitive and/or confidential information to users or the public who do not have authorization to receive this type of information. This error could compromise enforcement actions or disrupt the deliberative decision making or legal process for sensitive projects. The consequences will extend beyond the work performed to affect other Programs in the Department. The magnitude of this type of error is critical and could result in litigation against the Department. Given the confidential nature of DTSC's regulatory activities, the unauthorized release of sensitive information could also compromise national security.
2) Failure to ensure DTSC's compliance with control agency information security procedures and reporting requirements could jeopardize DTSC's credibility with the State Office of Information Security. The magnitude of this type of error is moderate and could tarnish the Department's reputation with control agencies and the Governor's Office.
3) Failure to properly report and/or monitor inappropriate employee behavior and misuse of systems and resources could result in embarrassment to OEIM and loss of credibility with customers. The magnitude of this type of error is moderate and could result in loss of productivity, increase in security vulnerabilities, and could contribute to an inappropriate work environment.
4) Failure to perform the duties described above, or failure to perform these duties correctly or in a timely manner could result in the inability of DTSC to meet regulatory commitments and to perform daily business activities. The potential impact ranges from minor inconveniences to DTSC staff to security impairments and mission critical activities. In addition, such failure could impact the Department's ability to ensure security, public safety and have negative financial impacts to DTSC.

G. Functional Requirements

The incumbent works most of the time on a desktop computer in a cubicle environment in a high-rise office building. A flexible work schedule, including telework, is available (the incumbent will be expected to be available through various platforms throughout the day to communicate on work related activities). The ability to use a personal computer and telephone is essential. No specific physical requirements are present. May be required to travel to meetings, training, and the regional offices. The incumbent may work with sensitive and confidential information. The incumbent must be able to meet critical deadlines.

H. Other Information

This position requires the ability to perform a variety of technical duties in support of the Department's IT systems. An expert understanding of networking technologies is required. Knowledge and skill in utilizing Microsoft PowerShell is desirable. Cisco Certified Internetwork Expert (CCIE) or equivalent in Security and/ Enterprise Infrastructure and the Palo Alto Network Certified Network Security Engineer (PCNSE) certifications are highly desirable. The incumbent must have good customer service skills and work well with others in a team environment.

I. DTSC's Equity Statement

The Department of Toxic Substances Control (DTSC) values diversity, equity, and inclusion throughout the organization. We foster an environment where employees from a variety of backgrounds, cultures, and personal experiences are welcomed and can thrive. We believe the diversity of our employees is essential to inspiring innovative solutions. Together we further our mission to protect California's people and environment from harmful effects of toxic substances by restoring contaminated resources, enforcing hazardous waste laws, reducing hazardous waste generation, and encouraging the manufacture of chemically safer products.

I have read and understand the duties listed above, and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with your supervisor.)

____________________________________ _______________________
Employee Signature Date

____
Printed Name

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

____________________________________ _______________________
Supervisor Signature Date

____
Printed Name

Approved Date: 9/2021