DUTY STATEMENT

☐**CURRENT** ☒**PROPOSED**

RPA Number: **25-OEIM-022**	Classification Title: **Information Technology Specialist III**	Position Number: **810-250-1415-002**
Incumbent Name:	Working Title: **Senior Cyber Security Operations Engineer**	Effective Date:
Tenure: **Permanent**	Time Base: **Full-Time**	Intermittent Hours Per Month:
Division/Office: **OEIM / HQ**	Section/Unit: Enterprise Information Security Branch / Enterprise Security Services Unit	Reporting Location: **Headquarters**
Supervisor's Name: **Richard Cabutage**	Supervisor's Classification: **Information Technology Manager II**	CBID: **M01**
Confidential Designation: ☐YES ☒NO	Designated Position for Conflict of Interest: ☒YES ☐NO	Position Telework Eligible: ☒YES ☐NO
Supervision Exercised: ☒None ☒Lead ☐Managerial ☐Supervisory		

Human Resources Use Only:		
HR Analyst Approval		
HR Analyst Name Alisha Hardy	HR Analyst Signature Alisha Hardy	Date 8/1/24

General Statement

This position requires the incumbent to maintain consistent and regular attendance; communicate effectively (orally and in writing if both appropriate) in dealing with the public and/or other employees; develop and maintain knowledge and skill related to specific tasks, methodologies, materials, tools and equipment; complete assignments in a timely and efficient manner; and adhere to department policies and procedures regarding attendance, leave, and conduct.

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.

Position Description

Primary Domain: Security Engineering; Secondary Domain: Systems Engineering Domain: Software Engineering. Under the administrative direction of the Information Technology Manager II of the Enterprise Information Security Services Branch, the Information Technology Specialist III (ITS III) will serve as the Senior Information Security Engineer. Performing Information Technology (IT) support functions that support and continuously improve DTSC's security posture, the incumbent 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:

Essential Functions (Including percentage of time):

25%	**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 subject matter expertise relating to security project efforts and infrastructure operations.
25%	**Cybersecurity Monitoring and Vulnerability Assessments** Performs complex cybersecurity event analysis in areas such as Spam/Phishing messages, Suspicious/malicious network, and system activity and Wireless (Wi-Fi) security. Performs advanced Cybersecurity Monitoring tasks including Threat Hunting, network forensics and malware analysis to proactively identify and mitigate potential security threats to an organization's network and system. Creates artifacts related to proactively identify and mitigate potential security threats to an organization's network and systems to document necessary information to provide support for incident response, investigations and compliance reporting. Communicates information related to Cybersecurity Monitoring to other security functions as well as external DTSC customers as needed. Conducts continuous vulnerability assessments of DTSC's systems, analyzes the results, advises IT staff, and communicates newly disclosed security vulnerabilities. Trains and mentors other SOC team members on process and procedures related to all SOC functions (i.e., Network Monitoring, Incident Response, and Administration.) Analyzes events related to Data Loss Prevention and identifies any potential needs for training, education, and awareness. Conducts security assessment exercises intended to identify security vulnerabilities or risk.
20%	**Information Security Architecture and Administration** 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, infrastructure security, threat hunting, etc. Applies knowledge of 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 configuration oversight. Provides Information Security Program planning assistance within the realms of security, forensic investigation, IT architecture, operations, system administration and security compliance.
15%	**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. Research,

	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.
5%	**Security Education and Training** Research and communicate 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%	**Administrative Duties** The incumbent is 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.

Marginal Functions (Including percentage of time):

5%	**Other related duties as required** Other related duties, as assigned within the classification of this position.

Typical Physical Conditions/Demands:

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.

Typical Working Conditions:

This position requires the ability to perform a variety of technical duties in support of the Department's IT systems. The incumbent must have good customer service skills and work well with others in a team environment. The incumbent will be interacting with various users and stakeholders of the Department's IT systems. This includes providing support and guidance to end-users, responding to inquiries or technical issues, and collaborating with other IT staff to ensure that issues are resolved in a timely and efficient manner. The incumbent must be able to communicate effectively, collaborate on problem-solving, and work together to achieve common goals. The IT Spec III is expected to have strong knowledge of various IT systems, including hardware, software, and networks. They must be able to troubleshoot and resolve technical issues that may arise in the course of their duties. They may also be responsible for performing routine maintenance and updates to various systems and ensuring that they are functioning properly.

Special Requirements of Position (Check all that apply):

☐ Duties performed may require pre-employment and/ or routine screenings (background/criminal/fingerprint clearance, drug testing, fingerprinting, physical, etc.).

☐ Duties require participation in the DMV Pull Notice Program.

☐ Performs other duties requiring high physical demand. (Explain below)

☐ Requires repetitive movement of heavy objects and/or operation of heavy machinery or motorized vehicles.

☒ Other (Explain below)

Explanation:

Action and Consequences

There are four areas in which there could be consequences to OEIM and/or the Department if the job is performed inadequately, including: 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. 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. 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. 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.

Supervisor Statement

I certify this duty statement represents an accurate description of the essential functions of this position. I have discussed the duties of this position with the employee and provided the employee a copy of this duty statement.

Supervisor Name	Supervisor Signature	Date

Employee Statement

I have discussed these duties with my supervisor and have been provided a copy of this duty statement. I certify I have read, understand, and can perform the duties of this position either with or without reasonable accommodation*.

**A Reasonable accommodation is any modification or adjustment made to a job, work environment, or employment practice or process that enables an individual with a disability or medical condition to perform the essential functions of his or her job or to enjoy an equal employment opportunity. (If you believe reasonable accommodation is necessary, check yes. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the Reasonable Accommodation Coordinator.)*

Do you need a reasonable accommodation to perform the essential functions of this position?	☐ **YES** ☐ **NO**

Employee Name	Employee Signature	Date