DUTY STATEMENT

☒CURRENT ☐PROPOSED

RPA Number: **HRC0001224**	Classification/CBID: **Information Technology Specialist II/R01**	Position Number: **810-250-1414-001**
Incumbent Name:	Working Title: **Cyber Security Engineer**	Effective Date:
Tenure: **Permanent**	Time Base: **Full-Time**	Intermittent Hours Per Month:
Program/Division: **OEIM**	Branch/Section/Unit: **Enterprise Security Services**	Reporting Location: **Headquarters (HQ)**
Supervisor's Name: **Richard Cabutage**	Supervisor's Classification: **IT Manager II**	Position Telework Eligible: ☒YES ☐NO
Confidential Designation: ☐YES ☒NO	Designated Position for COI: ☐YES ☒NO	Position Designated Bilingual: ☒YES ☒NO
Supervision Exercised: ☒None ☐Lead ☐Managerial ☐Supervisory		

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

Under the direction of the Information Technology Manager II (ITM II), the Information Technology Specialist II (IT Spec II) will serve as a Cloud Engineer. The IT Spec II performs complex Information Technology (IT) and oversight functions that support and continuously improve the Department of Toxic Substances Control's (DTSC) infrastructure. 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%	**<u>Information Security Operations and Services</u>** Maintains security components within DTSC's enterprise, including fulfilling security roles within Microsoft 365. Advises and participates in the creation of information security standards and

	standard operating procedures, while also analyzing new and existing cloud software application integrations to ensure compliance with security requirements. Collaborates with stakeholders to work on new cloud usage proposals and provide risk analysis for IaaS, PaaS, and SaaS offerings. Identifies risks, recommends, and deploys approved tools to automate security processes, and provide support for Technology Recovery Planning, by leveraging expertise in network and cloud security. Consults with stakeholders to assess business impacts and exposure for IT solutions, while utilizing management consoles, monitoring tools, and DTSC-owned security systems to identify potential indicators of compromise and vulnerabilities. Assists in the administration of DTSC security solutions, analyze incident-related data, respond to security requests, and actively support incident response activities.
25%	**Information Security Solutions** Advises, creates, and actively participates in the design of new system planning, standards, and methods to support the organization's technology strategies, which includes creating secure solutions, encompassing various aspects such as cloud deployments, host-based security implementation, system hardening, and the deployment of security services like remote access, penetration testing, security architecture, threat hunting, fraud detection, network security, scanning services, log management, and security monitoring/systems. Conducts audits and vetting software applications to ensure compliance with security requirements, and identifies security concerns to protect DTSC assets. Triages tool findings, summarizes them in high-level reports, and implements approved remediation measures, to maintaining a secure environment. Reviews code changes, provides input on addressing security issues, and deploys automation tools to augment security checks. Supports IT Contingency Planning, through participation in preliminary planning, business impact analysis, alternate site selection, recovery strategies, risk assessments, and training/exercises within the Business Continuity Plan framework. Collaborates with stakeholders to perform threat modeling and architecture risk analysis on new design proposals, ensuring security considerations are integrated throughout the project lifecycle.
20%	**Cybersecurity Incident Response** Conducts incident response activities, by effectively communicating and collaborating with DTSC's IT staff during the analysis and response to security events and engaging Security Management and the Chief Information Security Officer to provide timely updates and recommendation when high-risk and urgent security incidents arise. Generates comprehensive written reports and other necessary artifacts to document the investigation process leading to the incident response activity.
10%	**Cybersecurity System Technical Administration** Performs technical system administration tasks regularly for multiple security systems, to ensure proper maintenance and operation. Performs (non-security) incident response for issues impacting security system operation with DTSC end-user impact.
10%	**Information Security Compliance Oversight** Ensures the security of DTSC systems and their compliance with relevant requirements. Serves as a liaison between technology and business project teams to provide information security requirements and offer best practice guidance to ensure the fulfillment of compliance mandates. Tracks and documents non-standard software approvals to ensure comprehensive oversight of DTSC's software landscape and adherence to security requirements. Represent the Security Operations Center on special teams and projects. Creates, reviews and updates security alert, process, and procedure documents related to Cybersecurity Monitoring, Incident Response, Security Configuration Baselines and Technical Administration of systems. May serve as lead. Perform other related activities as specified by the Security Management Team.
5%	**Administrative Duties** Performs administrative duties including but not limited to the following 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 time sheets by the due date.

Marginal Functions (Including percentage of time):	
5%	**Information Technology Projects/Other Related Duties** Other related duties, as assigned within the classification of this position.

Consequences of Error: (if applicable)

Typical Physical Conditions/Demands:

The work typically requires sitting for prolonged periods while reading, writing, typing, and participating in meetings. The position requires bending and stooping. The job requires extensive use of a personal computer and the ability to sit/stand at a desk, utilize a phone, and type on a keyboard for extended periods of time. It may be required to stand, bend, squat, reach, grasp and pick up items consistent with office work. The incumbent may be required to lift XX pounds and occasionally stand, bend, squat, reach, grasp, or kneel for long periods.

Typical Working Conditions:

Works in multi-story building, in a cubicle office setting using a variety of office equipment, e.g., computers, telephones, copiers, etc., with artificial light and temperature control, and attends meetings in similar settings. On an as-needed basis, work outside normal work hours, including evenings and weekends, may be required. A telework schedule may be available (the incumbent will be expected to be available through various platforms throughout the day to communicate on work related activities). The work schedule is Monday through Friday. Travel may be required locally and within the state. If travel is required, it will be by commercial carrier or auto, whichever method is in the best interest of the State. This position will have daily contact with DTSC staff, external state, and federal agencies, and local government representatives, and the public either in person, via email/telephone, or videoconferencing.

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:

Personal Contacts: The incumbent has daily contact with all levels of DTSC staff and management and must communicate the most complex technical and business process risks and issues to Executive staff. These contacts will frequently involve confidential and sensitive information regarding personnel, enforcement, and legal activities. The incumbent will have regular contact with

vendors and contractors, as well as occasional contact with other State departments, local government organizations, and external stakeholders.

Actions 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 deliberate 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 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 on the Department's ability to ensure security, public safety and have negative financial impacts on DTSC.

Other Information: This position requires the ability to reason logically and creatively, develop and evaluate alternatives, analyze data, effectively communicate ideas and information, and effectively gain and maintain the confidence and cooperation of those contacted during work. The incumbent must exhibit punctuality and dependability in executing the duties of this position. The incumbent must possess knowledge and skill in the SDLC as it applies to IT, business process re-engineering, as well as administering and supporting an enterprise IT telecommunications environment. The incumbent must have good customer service skills and work well with others in a team environment.

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

HUMAN RESOURCES BRANCH USE ONLY:

☒ Duties meet class specifications and allocation guidelines.

☐ Exceptional allocation, STD 625 on file.

Analyst initials: SB Date Approved: 5/12/2026

Revision Date (if applicable): Click or tap to enter a date.