Department of Toxic Substances Control
Position Duty Statement

Classification Title Information Technology Specialist III	**Department** Department of Toxic Substances Control
Working Title Information Security Officer	**Office/Unit/Section/Geographic Location** Office of Environmental Information Management / Sacramento Headquarters' Office
Position Number 810-250-1415-XXX	**Effective Date** June 12, 2020
Domain IT Security	

General Statement: Under the administrative direction of the Deputy Director, the Information Technology Specialist III (IT Specialist III) performs all functions in the role as the Department of Toxic Substances Control's (DTSC's) Information Security Officer (ISO). The IT Specialist III is responsible for directing, planning, controlling, and implementing information security practices throughout the Department's Information Technology (IT) and business technology infrastructure to ensure that DTSC is in compliance with all applicable statutory, regulatory, and control agency security standards. The incumbent directs the planning and implementation of enterprise IT system, business operation, and Departmental IT infrastructure against security breaches and vulnerability issues. The incumbent is also responsible for auditing existing systems, and administering security policies, activities, and standards. The incumbent is responsible for working with CalEPA's Agency Information Security Officer (AISO) to ensure Agency IT security policies and direction are adhered to and applied to DTSC programs, strategic goals, and business objectives. The incumbent is assigned sensitive and technically complex assignments as described below. Duties include, but are not limited to:

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

25% (E) Policy and Program Management
Directs, plans, organizes, and controls the Department's implementation of the information security program including practices and procedures required by the California Technology Agency's Office of Information Security (OIS), National Institute of Standards and Technology (NIST), and System Administration Networking and Security (SANS) to ensure that all deployments, enhancements, operations, and maintenance of DTSC's network systems are documented and in compliance with control agency security standards. Protects DTSC's information and information processing assets by ensuring that DTSC is in compliance with all applicable legal, statutory, and regulatory requirements concerning information security management and best business practices. These activities include but are not limited to: directing the preparation of disaster and technology recovery plans; investigating, resolving, and reporting information security incidents; ensuring compliance with telework and remote access security standards and social media standards; developing security management plans consistent with State Administrative Manual (SAM) Chapter 5300; and ensuring IT security certifications are submitted according to control agency requirements. This work includes submitting certain security documents, including disaster recovery plans and incident reports, to the California Technology Agency and the California Highway Patrol on an annual basis and during security incidents. Directs the reporting of security metrics using methodologies developed by the State OIS. Participates in activities coordinated by the OIS in order to better understand and address security incidents and critical cyber security threats to the State.

25% (E) Risk Management and Incident Response
Develops, implements and manages risk management plans consistent with State Administrative Manual (SAM) Chapter 5300 including but not limited to risk management, audit and compliance, information security governance, incident management program, and continuity of operations and

government programs. Manages information security vulnerabilities within DTSC's information processing infrastructure. Information security vulnerabilities could be discovered in DTSC's IT applications, operating systems, and networks with the potential to expose sensitive information. Directs advanced oversight and system guidance, as well as technical security support for all enterprise infrastructure that supports business functions. This work includes directing the analysis of new releases of OS software to ensure they meet established baseline standards set forth by DTSC, CalEPA, OIS, SANS, and other recognized security organizations. Directs, monitors and reviews central anti-virus reporting and virus incidents, as needed, to troubleshoot and refer actions associated with inappropriate use of computing systems and improving anti-virus mitigation and protections. Directs monitoring of DTSC's network traffic on a regular and periodic investigative basis, including monitoring and analysis of web reporting systems for security threats that include unauthorized access and employee inappropriate activity. Responsible for intrusion detection and prevention system (IDPS) traffic for anomalies and responds to alerts including conducting ad-hoc computer security incident reviews and computer vulnerability assessments for the identification and detection of high-risk and/or suspect activities and/or vulnerabilities (i.e., potential of resident malware; un-patched desktop computers and servers). Directs and performs vulnerability assessments of new and existing systems to ensure vulnerabilities and deficiencies are remeidated. Provide leadership, direction and guidance in assessing and evaluating information security risks and monitor compliance with security standards and appropriate policies.

20% (E) Security Oversight and Strategic Planning Management

Provides consultation and recommendations to resolve the most complex information and physical security issues. Develops and implements plans to streamline and improve policies, procedures, standards, and guidelines, which will enhance DTSC's overall security position. Directs the implementation of new security controls to be able to more effectively monitor DTSC's IT infrastructure and information systems for inappropriate use or unauthorized activity. Directs the change management process to ensure that all changes to the enterprise systems or services are conducted in a controlled manner and properly documented. Demonstrates a broad understanding of enterprise policy, procedures, standards, and guidelines and their effect on the business environment and criticality to DTSC's mission. Collaborates with the State CISO to ensure alignment with statewide information security initiatives, leads and participates in security planning sessions. Researches and evaluates current and new security technology and trends to develop an information security architectural roadmap. Conducts maturity assessments to identify gaps and develop alternatives for investment recommendations to improve DTSC's security posture in workforce qualifications, system and technical architecture, and business processes. This work may involve comparing baseline information in certain subject areas such as technology, system users, or IT processes, against control agency requirements as mandated by OIS, CalEPA AISO, SANS, NIST, and any other information security organizations.

15% (E) Shared Technology Environment

Provides information security updates to CalEPA's AISO for DTSC systems to ensure information security policies and standards are being met. Works in partnership with CalEPA's AISO on information security activities related to CalEPA's shared environment. Collaborates with CalEPA's AISO and Departmental executives and senior managers to integrate administrative security controls into business processes and procedures.

10% (E) Security Awareness, Education, and Training

Directs the education/training of DTSC employees about their security and privacy protection responsibilities. Directs system administrators and application developers to develop installation and deployment plans for all software and hardware. This includes directing system administrators to ensure that critical patches are deployed in an acceptable time frame to avoid a security vulnerability. Directs staff in performing informal and formal security reviews, assessments and audits for DTSC's local area network and wide area network (LAN/WAN) environments, as well as, other contract and regional partner networks and systems. Conducts and documents information security awareness training for all Departmental employees on an annual basis. Directs, prepares, and provides oversight and delivery of training, presentations,

and briefings for Executive staff and various discrete audiences and venues on information security issues.

5% (E) Administrative Duties
Performs 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.

B. Supervision Received
The IT Specialist III reports directly to the Deputy Director (Chief Information Officer), a Career Executive Assignment B (CEA B), within the Office of Environmental Information Management. The IT Specialist III receives general direction and most assignments from the Deputy Director. The IT Specialist III may also receive general direction from the AISO, Agency Information Officer (AIO) and the Secretary of CalEPA on cross BDO security policies and activities. The IT Specialist III directs the IT security activities of OEIM staff, and acts as a team leader on the more complex information security projects. The IT Specialist III also works independently as a high-level technical specialist on the more complex IT security assignments.

C. Supervision Exercised
Although the IT Specialist III will not be the direct supervisor of staff, the incumbent will be responsible for directing security related activities being performed by various technical OEIM staff. The IT Specialist III will be responsible for training, coaching, mentoring, and leading staff in OEIM to ensure that all information security practices throughout the Department's IT and business technology infrastructure are in compliance with applicable legal, statutory, and regulatory requirements, including State control agency security standards.

D. Administrative Responsibilities for Supervisors and Managers
Although the IT Specialist III is a non-supervisory position, the incumbent does have direct administrative responsibilities for the operational control of all DTSC-wide oversight of security measures and activities. The incumbent manages critical security aspects of DTSC's business technology infrastructure and IT security practices.

E. Personal Contacts
The IT Specialist III directs the activities of advanced technical disciplines and/or areas of management, including vendor system experts, systems and network administrators, database system administrators, server application developers, multiple programs within DTSC, project team members, peers, other Agency and State Information Officers, and other external consultants, contractors, and vendors. The IT Specialist III collaborates with the AISO, Agency Information Officer and other CalEPA BDO executives and senior managers to integrate administrative security controls into CalEPA and Departmental processes and procedures.

F. Actions and Consequences
There are five 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 work with the AISO to properly provide security oversight activities, including enterprise disaster recovery planning, enterprise risk management and incident response could result in significant detrimental statewide impact and compromise information of CalEPA and its BDOs. The consequence of error (lack of policy enforcement, Agency disaster recovery planning, risk management, and incident response) is critical and could result in security risk exposure, electronic terrorism, and liability to the State.

3) 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.

4) Failure to properly 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.

5) Failure to conduct information security awareness training and education to OEIM staff and all other Departmental staff could result in the compromise of sensitive and/or confidential information. The magnitude of this type of error is moderate and could jeopardize the integrity of data.

G. Functional Requirements

The incumbent works primarily on a desktop computer in a cubicle environment in a high-rise office building in downtown Sacramento. The incumbent may spend multiple hours a day on the phone or in meetings, interacting with customers, management and staff on detecting, reporting, and mitigating security breaches, intrusions, and employee misuse of systems and resources. The incumbent may work on sensitive, confidential and controversial assignments. The incumbent must work well with others, accommodate changing priorities, work occasional irregular or overtime hours, and be able to meet critical deadlines. The incumbent will use a variety of office equipment, (e.g., computers, copiers, digital senders, videoconference equipment, etc.).

H. Other Information

This position requires the ability to plan, coordinate and direct the activities of data processing and other technical staff; develop and evaluate alternatives; make decisions and take appropriate action; establish and maintain priorities; effectively develop and use resources; analyze data and effectively communicate ideas and information to staff and management; reason logically and creatively and use a variety of analytical techniques to resolve managerial problems; and successfully gain and maintain the confidence and cooperation of those contacted during the course of work. The incumbent may be required to travel up to 5% of the time (by automobile, rail, or air) to DTSC Regional Offices or remote field sites. This travel would be based on need to respond to IT security incidents, security audits, or to oversee or conduct user training, and would not be for periods longer than a week. The incumbent must exhibit punctuality and dependability in executing the duties of this position.

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: August 24, 2020 ML