DUTY STATEMENT ☒CURRENT ☐PROPOSED

RPA Number: 24-OEIM-348	Classification Title: Information Technology Manager II	Position Number: 810-250-1406-001
Incumbent Name:	Working Title: Deputy Chief Information Officer	Effective Date:
Tenure: Permanent	Time Base: Full-Time	Intermittent Hours Per Month:
Division/Office: Headquarters	Section/Unit: OEIM / Enterprise Security & Infrastructure Services Branch	Reporting Location: Sacramento HQ
Supervisor's Name: Don Foley	Supervisor's Classification: CEA	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 Monica Vasquez	HR Analyst Signature Monica Vasquez	Date 3/19/24

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

Operations in partnership with OEIM Senior Management, DTSC and Agency personnel. The Information Technology Manager II (ITM II) is responsible for leading and managing the Enterprise Security and Infrastructure Services branch and complex information technology projects. Responsibilities include advising and communicating to the Chief Information Officer (CIO), DTSC executives, division chiefs, program managers, and Agency management on all matters related to the implementation and impact of IT systems and security across lines-of-business activities and the tactical implementation of the IT strategy, processes and methodologies as defined by the CIO. Establish vision, goals, objectives, strategies, and tactical direction for Multi-Cloud and Data Center technologies, Enterprise Security and Infrastructure operations, OEIM Service Level agreements and key performance indicators, and management of OEIM Operational Project Portfolio. The ITM II may act on behalf of the CIO in their absence, utilizing established authority provided by DTSC executive staff. Specific duties include but are not limited to:

Essential Functions (Including percentage of time):

40% **OEIM Operations, Enterprise Security and Infrastructure Operations Management**

Under the direction of the CIO, deliver a clear technology vision, providing strategy and direction to Enterprise Security and Infrastructure Services branch by setting goals, expectations, encouraging leadership, teamwork, collaboration, transparency, and motivating staff at all levels. A supporter and advocate of DTSC's core values, OEIM's team first culture, and customer service-oriented communication and service delivery standards. Promote Department and Agency mission, goals, objectives, policies, processes, and procedures. Direct and oversee OEIM daily operations and production services, including change control, change management, fiscal management, contract management, operations management, resource management and talent management. Plan, organize, and direct the multidisciplinary teams of IT professionals, and manage the workload and resources through subordinate managers and leads. Ensure appropriate staffing levels and skills are assigned to maintain efficient and effective operations to support ESIS service offerings within budgeted resources. Responsible for the resource planning of the work activities related to enterprise security and infrastructure services, including but not limited to: Client Services and Support, Infrastructure Services (Network, Servers, Storage, Wireless capabilities), Telecommunications, IT Asset Management, Multi-Cloud, Data Center and hybrid Technologies, Security Services and Operations, IT Risk Management; Information Security Compliance Management; Incident Management; Privacy and Security Awareness Program; Technology Recovery Planning; and Security Control Audit Program. Implements infrastructure and security strategies and tactical best practices, determined generally by industry best practices, in collaborative partnership with OEIM Management, DTSC and CalEPA (Agency). Evaluates, plans, and determines key performance indicators and develop work plans to increase efficiencies of OEIM's Operations and service levels for enterprise infrastructure and security services. Provides direction on organization's contingency plans for business continuity and continual process improvements. Oversees continuous monitoring of all enterprise security and infrastructure services for technology changes, topology changes, anomalous activity, and other alterations that might impact DTSC business operations. Lead and manage OEIM Operational Project Portfolio in collaboration with OEIM Senior Management and personnel for program prioritization.

15% **Service, Risk and Compliance Management & Privacy Program Oversight**

Identifies infrastructure and security risks, manages the risk register, and works with System Owners to mitigate identified and future risks throughout the Department. Oversees departmental risk assessments, both internal and external triggered, identifying potential vulnerabilities and its business impact that threaten the security, confidentiality, and integrity of DTSC information assets. Collaborates throughout the Department to identify and estimate the cost of protective measures to mitigate and prevent vulnerabilities to an acceptable level. Participates in the selection of cost-effective security management measures and tools to mitigate security threats. Prepares confidential reports for OEIM Senior Management documenting identified risks, proposed security management measures, resources necessary for security management and residual risk. In collaboration with the Privacy Office, serves as the subject matter expert on privacy policy recommendations, development, reviews and updates. Performs complex business process analysis to ensure enterprise systems and business areas incorporate privacy principles and requirements in accordance with state and Federal mandates. Oversee and support the Privacy Program by identifying privacy weaknesses and propose solutions to appropriate project, IT, or program management. Reviews and updates existing processes for

	privacy compliance with statewide privacy policies. Identifying privacy compliance issues and supports system owners/custodians in remediation development in compliance with State of California, Agency and DTSC's privacy policies. Handles privacy incidents, completes all facets of the incident response, including, but not limited to, conduct interviews, draft reports, document lessons learned, and address privacy risks or issues in order to resolve incidents in a timely manner and from this data, identifies needed improvements in the design, implementation, and operation of DTSC's privacy program.
15%	**Infrastructure, Security Program, and Policy Management** Develops, implements, and manages the DTSC's information security program that supports business operations and aligns with the departmental mission, goals, and objectives. Ensures the information security program is compliant with all applicable legal, statutory, and regulatory requirements. Work in collaboration with Chief Information Security Officer (CISO) to identify and improve enterprise infrastructure and security posture, thru security management frameworks such as NIST, FEDRAMP, FIPS, OWASP and SIMM. Serving in partnership with the OEIM Senior Management, establishes security and infrastructure strategy, roadmap(s), and information technology policy for DTSC. Formulates, recommends, and oversees implementation of the Department's enterprise-wide information technology security policies and standards. Oversees and/or directs the implementation of information security policies and practices related to the delivery and protection of information assets. Ensures that the Department is in compliance with State, Agency and DTSC information security policies, standards and requirements. Provides oversight over all information technology security operational activities within the DTSC. Collaborates with departmental executives and senior managers to integrate administrative security controls into Department processes and procedures. Works with various programs to ensure that staff and management comply with the information security policies, standards, and other applicable requirements. Assists, or leads, planning related to emergency preparedness, incident response, and prevention.
10%	**Personnel Management** Plans, organizes, directs, and provides managerial review of the work performed in the Branch. Provides regular and timely written performance appraisals to staff. Counsels staff and initiates disciplinary actions as necessary. Recruits, hires, trains, develops, and provides leadership to staff. Complies with state and federal laws, rules, regulations, bargaining unit contracts, and policies in all personnel practices. Manages and coordinates assignments of technical staff based on departmental and OEIM priorities, staff experience and skill levels, complexity assessments of projects, specialized skills and experience requirements, and resource availability. Establishes performance standards and expectations by conducting probationary reviews, annual performance reviews, annual Individual Development Plans, constructive intervention, corrective and disciplinary actions, and training to enhance personnel growth. Establishes reasonable deadlines and monitors staff's workload to ensure work is completed accurately and timely. Provides advice and consultation to staff on the most difficult and sensitive work issues. Encourages team building across all service delivery teams. Facilitates cross training and promotes continuous improvement of processes. Implements motivation techniques, promotes training, and creates a positive climate for change. Mentors staff and ensures training opportunities are available to assist in developing technically skilled staff. Sets and communicates standards of performance for all team members. Promote upward mobility and provide equal employment opportunities for a harassment and discrimination-free work environment. A catalytic agent in developing a customer focused service organization.
10%	**Research and Training** Researches and evaluates current and new infrastructure and security technologies and trends. Collaborates with Agency and BDO (Boards, Departments, Offices) IT enterprise architects, and information security teams to assist with the design, implementation and identifying standards for infrastructure and security technical controls or threat countermeasures for projects, systems, and applications. Conducts infrastructure and security assessment to identify gaps and develop alternatives for investment recommendations to improve enterprise-wide security posture in system and technical architecture, and business operations.

5%	**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.
Marginal Functions (Including percentage of time):	
5%	**Team Leadership** As a member of the OEIM's leadership team, participates in organizational efforts to facilitate the effective management and leadership of the organization. Performs other related duties, as required.

Typical Physical Conditions/Demands:

The job requires extensive use of a personal computer and the ability to sit/stand at desk, utilize a phone, and type on a keyboard for extended periods of time.

Typical Working Conditions:

The ITM II works in a high rise building with artificial light and temperature control. 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. May be required to travel to meetings, training, and the regional offices. The incumbent may work on sensitive, confidential, and controversial assignments. The incumbent must work well with others, accommodate changing priorities, work occasional irregular or extended hours, and be able to meet critical deadlines.

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:

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