DUTY STATEMENT

Employee Name:	

Classification:	Position Number:
Information Technology Manager II (Information Security Engineering)	580-150-1406-XXX
Working Title:	Work Location:
Chief Information Security Officer	1616 Capitol Avenue Sacramento, CA 95814
Collective Bargaining Unit:	Tenure/Time Base:
M01	Permanent/Full-time
Center/Office/Division:	Branch/Section/Unit:
Information Technology Services Division	Information Security Office

All employees shall possess the general qualifications, as described in California Code of Regulations Title 2, Section 172, which include, but are not limited to integrity, honesty, dependability, thoroughness, accuracy, good judgment, initiative, resourcefulness, and the ability to work cooperatively with others.

This position requires the incumbent to maintain consistent and regular attendance; communicate effectively (orally and in writing) 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 departmental policies and procedures.

Job Summary

Under administrative direction, serves in an executive managerial level position as the California Department of Public Health's (CDPH) Chief Information Security Officer (CISO). The CISO serves as principal information security policy and governance advisor to the Director's Office, Program Deputy Directors, and the Information Technology Division Deputy Director. The CISO manages the enterprise Information Security Office (ISO) Program. The ISO is statutorily mandated by law to safeguard the confidentiality, integrity and availability of state information, systems, and applications to promote and protect the development of information technology infrastructure and networks, and ensure the uninterrupted operation of mission critical CDPH and affliated State programs.

The CISO serves in an executive management role in setting, influencing and directing the security aspects of the initiation, design, development, testing, operation, and defense of information technology data and environments to address sources of disruption, ranging from natural disasters to malicious acts. The CISO is the primary information security point of contact for external agencies including the CA. Highway Patrol; CA. Department of Military; CA. Department of Technology; CA. Health and Human Services Agency; CA. Office of Health Information Integrity; CA. State Auditor; CA. Office of Emergency Services-Homeland Security Division–Cybersecurity Integration Center; the U.S. Federal Bureau of Investigation; the U.S. Social Security Administration; the U.S. Health and Human Services Agency-Office for Civil Rights-Health Insurance Portability and Accountability Act compliance; the U.S. Centers for Disease Control; and others. Thru affiliated managers and supervisors, the CISO coordinates and directs information security protection and compliance activities with the Security Operations Center and multiple data center management units. Thru affiliated managers and supervisors manage the security aspects of the initiation, design, development, testing, operation and defense of information technololgy data and environments to address sources of disruption, ranging from from natural disasters to malicious acts.

The CDPH Business Continuity Plan identifies the CISO as one of two positions that are authorized to direct the activities of the Information Technology Services Division in the event that the Deputy Director for the Division is unavailable in emergency scenarios. The CISO is tasked with effectively promoting equal opportunity in employment and maintaining a work environment that is free of discrimination and harassment in order to

effectively contribute to the Department's Equal Employment Opportunity objectives. The CISO will periodically travel to the CDPH Richmond campus and/or other facilities as required. The ITM II will work in the Information Security Engineering Domain.

Special Requirements

- ☐ None
- ☒ Supervision Exercised
- ☒ Conflict of Interest (COI)
- ☐ Background Check and/or Fingerprinting Clearance
- ☐ Medical Clearance
- ☒ Travel: Upto 5% travel to the CDPH Richmond campus and/or other facilities may be required.
- ☐ Bilingual: Pass a State written and/or verbal proficiency exam in
- ☐ License/Certification:
- ☐ Other:

Essential Functions (including percentage of time)

35% Development and executive oversight of the CDPH cybersecurity framework with activities that cross agency, departmental, office, functional, and project boundaries. CDPH decision-making authority for information security compliance, affecting approximately 3,600 staff engaged in 200 separate lines of business supporting the CDPH Mission of “Advance the health and well-being of California's diverse people and communities”. Consider the impact of actions and make challenging and appropriate decisions to support the Information Security Program.

Supervise, manage, and lead the Information Security Office. Develop policy, programs, and guidelines for implementation. Ensure the ISO workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. Review/Assess the competencies of the Information Technololgy Manager and Information Technology Specialist security staff.

Review, analyze and approve CDPH purchase orders and contracts that have information technology components for security impacts.

Broad responsibility for implementation and extensive participation in policy evolvement of the Departmental information security policy. Decision-making authority for the development, maintenance, implementation and enforcement of CDPH policies, procedures, practices, standards, security directives, and guidelines, and the Organizational Change Management and Business Process Improvement integration strategies to support these administrative controls, that ensure the consistent and comprehensive conformance of information security throughout CDPH and it’s external public and private data sharing partners and contractors.

Develop and implement information security education programs that are key in the creation of a culture that places a high value on the security of CDPH information, information assets, and the protection of personal information. Develop and implement specific training for staff with significant information security or systems access. Provide guidance and expert knowledge to senior CDPH executives regarding IT security policies and responsibilities.

25% Develop, establish and administer the Enterprise information security risk management policy and strategic direction. Conduct and coordinate information resource security and risk assessments and monitoring activities to identify vulnerabilities, threats, and risks within CDPH and outside data custodian environments. Make recommendations or direct effective and economical solutions and strategies that meet regulatory requirements to address those threats, risks, and vulnerabilities. Maintain an acute understanding of risk management concepts and best practices.

Review project plans and system architectures of new or modified information systems and ensure the incorporation of security standards and controls into the system development life cycle phases, and provide definitive reference points for validation, verification and audit activities. Review written certification that technology assets meet security requirements and issue accreditation approvals.

Coordinate the monitoring of CDPH's information technology physical security to identify threats to information assets, including personnel access to restricted areas, security of mobile computing equipment, access procedures and, provide recommendations or direct corrective action as needed.

Direct and coordinate the information classification processes for Business Continuity Planning, Disaster Recovery, Continuity of Operations / Continuity of Government, and Operational Recovery Planning. Direct and coordinate business impact assessments and risk analysis for critical business functions and systems. Recommend and direct the implementation of appropriate data backup and retention processes. Serve in the Emergency Operation Center as necessary. Coordinate the preparation, completion, validation and, scheduled testing of disaster recovery and business continuity documents, and their filing with control agencies and propagation to relevant CDPH management.

20% Full responsibility for the development and implementation of appropriate policies and strategies to manage security incidents and coordinate investigative activities. Act as a focal point for the Department's security investigations and when necessary, direct a full investigation with recommended courses of action and corrective action plans. Direct and advise departmental management and data owners through the formal incident response process including audit trail reviews. Submit required reports and documentation to control agencies.

Develop and sustain successful working relations with the Office of Legal Services, Privacy Office, Office of Compliance, Human Resources Branch, and Oversight Agencies to provide a comprehensive umbrella of privacy and security controls, investigative resources, and Public Records Act resources for CDPH.

Sponsor forums for communication of information security related activities, concerns and regulations impactful to CDPH operations. Function as the expert policy advisor for the CDPH Directorate's Information Security Governance Committee. Coordinate information security plan and program actions with the CDPH Executive Staff, Information Technology Services leadership, and relevant oversight agencies to assure uniform interpretation of security policy.

Lead and serve on CDPH committees responsible for the security and privacy oversight of data and information management systems and those projects that develop or impact those systems.

Provide required reports to control agencies on the implementation of CDPH's information security program and ongoing compliance with the State's security and risk management policies. Serve as the CDPH point-of-contact for control agency information security assessments and audits.

Officially represent CDPH to other State and Federal Agencies, and at external security conferences, forums and meetings. Advise and educate executive staff and division management regarding federal

and state security requirements and industry best practices for the proper classification, use, and protection of CDPH's information systems and data assets. Continually update working knowledge of the latest information and privacy security tools and concepts.

15% Manage the technical and administrative operations of the Information Security Office including but not limited to; personnel administration; contracts and purchasing; budgeting; training plans; Budget Change Proposals; consultant engagement and management.

Marginal Functions (including percentage of time)

5% Performs other work related duties as assigned .

I certify this duty statement represents an accurate description of the essential functions of this position. I have discussed the duties and have provided a copy of this duty statement to the employee named above.		I have read and understand the duties and requirements listed above, and am able to perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation may be necessary, or if unsure of a need for reasonable accommodation, inform the hiring supervisor.)	
Supervisor's Name	Date	Employee's Name	Date
Supervisor's Signature	Date	Employee's Signature	Date
HRB Use Only: Approved By: Byron Bennett	Date 11/23/20		