CALIFORNIA DEPARTMENT OF HUMAN RESOURCES

Duty Statement
Department of Human Resources
State of California

☒ Current ☐ Proposed

Classification Title	**Division/Unit**
Information Technology Manager I	IT Division
Working Title	**IT Domain** (if applicable)
Chief Information Security Officer	Information Security Engineering
Position Number	**Effective Date**
363-175-1405-XXX	
Name	**Date Prepared**

CalHR Mission and Vision

The California Department of Human Resources (CalHR) is responsible for issues related to employee salaries and benefits, job classifications, civil rights, training, exams, recruitment and retention. For most employees, many of these matters are determined through the collective bargaining process managed by CalHR.

Our Vision: To be the premier leader and trusted partner in innovative human resources management.

Our Mission: To provide exceptional human resources leadership and services with integrity, respect and accountability to state departments and all current and prospective employees.

General Statement

Under the general direction of the California Department of Human Resources (CalHR) Chief Information Officer (CIO), the incumbent serves as the CalHR and State Personnel Board (SPB) Chief Information Security Officer (CISO) who is responsible and accountable for the Department's Information Security and Privacy Programs that safeguard CalHR's information technology infrastructure and minimize cybersecurity threats against its network, systems, solutions, and data. This role also oversees the adoption, and implementation of regulations, laws, policies, frameworks, controls, standards, processes, and procedures related to information security across CalHR and SPB. In addition, the incumbent supervises and mentors the information security team. Duties include, but are not limited to, the following:

Job Functions

[Essential (E) / Marginal (M) Functions]:

Percentage (%)	**(E) or (M)**	**Job Duties**
30%	**(E)**	Proactively develops, implements and administers CalHR's and SPB's Information Security and Privacy Programs consisting of information security and privacy policies, architecture, frameworks, controls, standards, plans, processes, and procedures to comply with laws and regulations. Strategically manage risks relating to information and physical security, digital assets, technology recovery, and privacy.

20%	**(E)**	Supervises and mentors CalHR's Information Security Office (ISO) team, assigns tasks, and oversees day-to-day information security operational activities which include but are not limited to drafting policies and plans, reporting information security incidents to oversight agencies, coordinating audits with external and internal entities and all aspects of Risk Management e.g., - analysis, assessments, preparation, and reporting. Oversees ongoing risk assessments and audits to identify potential vulnerabilities in existing systems that could threaten the security, confidentiality and integrity of CalHR's and SPB's information assets. Ensures that CalHR follows California Department of Technology's (CDT) Office of Information Security (OIS) requirements and compliance reporting schedule including Designation Letters, Business Continuity Plans, Technology Recovery Plans, Incident Reporting, Risk Registry, and Plan of Action Milestones (POAM) and report all activities to the CalHR's Agency Information Security Officer.
20%	**(E)**	Monitors and oversees the updating of existing security and privacy policies, architectural, frameworks, controls, standards, plans, processes, and procedures based on legislation, State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), CDT Technology Letters, Management Memos, National Institute of Standards and Technology (NIST) Special Publications, Cybersecurity Frameworks, Critical Security Controls, Federal and State Privacy Acts, and industry best practices pertaining to the field of Information Security and Privacy. Ensures that all information security and privacy incidents are reported through the CDT California Compliance and Security Incident Reporting System (Cal-CSIRS) and per the California Department of General Services (DGS) SAM5300 and Information Security and the CDT SIMM 5300. When applicable, report all incident activities to California Office of Emergency Services (CalOES), California Military Department (CMD), CDT, and California Highway Patrol (CHP).
10%	**(E)**	Oversees and conducts in-person and online information security awareness and privacy training for all CalHR staff and contractors; documents and reports training compliance metrics to CalHR Executives.
10%	**(E)**	Develops information security performance metrics, reports information security risks, and shows policy gaps as well as opportunities for improvement with executives and applicable CalHR stakeholders.
10%	**(E)**	Represents the CalHR ISO in technology-related meetings and projects involving internal and external stakeholders.

Supervision Received
The Chief Information Security Officer reports directly to and receives the majority of assignments from the Chief Information Officer; however, direction and assignments may also come from the Executive Office.

Supervision Exercised
The Chief Information Security Officer directly supervises the following classifications: Information Technology Associate and provides indirect supervision and guidance to other Information Technology and Generalist classifications in the IT Division.

Special Requirements / Desirable Qualifications
The incumbent must apply a prominent level of organizational understanding to strategically manage risks related to information and physical security, digital assets, technology recovery and privacy.

Knowledge of: Analytical procedures and methods; the functions of California State Government, including the principles, practices, and policies of the California Office of Information Security and Privacy Protection; the development of security policies and procedures, security awareness programs, business continuity, disaster recovery plans, and operational recovery plans. Knowledge of the National Institute of Standards and Technology (NIST) 800-53 framework.

Ability to: Effectively communicate, both verbally and in writing, across all levels of management and the user community; develop clear, accurate, concise reports, correspondence, issue papers, memorandums, and other types of written communication to document security concerns and decisions; present such reports before IT management; network and interface effectively with business and technical personnel and communicate clearly to groups with multiple levels of IT knowledge; demonstrate strong interpersonal skills; provide technical guidance for lower-level staff and State contractors/consultants, and apply technical knowledge effectively.

Working Conditions
The duties of this position are performed indoors. The employee's workstation is located at 1515 "S" Street building and is equipped with standard or ergonomic office equipment, as appropriate. Telework is also available. Travel may be required to attend meetings or training classes.

Attendance
Must maintain regular and acceptable attendance at such level as is determined at the Department's sole discretion. Must be regularly available and willing to work the hours the Department determines are necessary or desirable to meet its business needs.

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 the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the RA Coordinator.)

*****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 their job or to enjoy an equal employment opportunity.

Duties of this position are subject to change and may be revised as needed or required.

Employee Signature	Employee Printed Name	Date

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	Supervisor Printed Name	Date