

**ESSENTIAL FUNCTIONS DUTY STATEMENT**

HRM-025

<b>Classification Title:</b> Information Technology Manager 1	<b>Branch/Division/Bureau:</b> Executive Operations/Enterprise Planning, Risk & Compliance
<b>Working Title:</b> Chief Information Security Officer	<b>Office/Unit/Section/Geographic Location:</b> Information Security Office/Sacramento
<b>Position Number (13 Digit):</b> 413-109-1405-001	<b>Conflict of Interest Position:</b> <input type="checkbox"/> NO <input checked="" type="checkbox"/> YES
<b>Employee Name:</b>	<b>Effective Date:</b>

**BASIC FUNCTION:**

Under general direction of the Enterprise Planning, Risk and Compliance Chief, CEA A, the Chief Information Security Officer (CISO) provides leadership, management direction, policy guidance, and oversees implementation of information security practices throughout the Department. This position has broad authority and responsibility for protecting the privacy, confidentiality, integrity, and availability of CDI information and services. The incumbent develops, implements, and maintains enterprise policies, standards, procedures, and guidelines for information security management to ensure the security, confidentiality, integrity, availability, and privacy of California Department of Insurance (CDI) information assets. The CISO works closely with the Information Technology Division (ITD). The ITD provides the technology solutions and services that support the CDI lines of business. The incumbent is assigned sensitive and technically complex assignments as described below.

The position requires the incumbent to travel up to 20% of the time.

This position is designated under the Conflict of Interest Code. The position is responsible for making or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete Form 700 within 30 days of appointment. Failure to comply with the Conflict of Interest Code requirements may void the appointment.

**ESSENTIAL FUNCTIONS**

**35%** Administers a comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, and privacy of information assets owned and controlled by CDI. Develops, implements, and manages CDI's information security components including, risk management; audit, and compliance; information security governance; incident management program; security awareness education and training; and continuity of operations and government programs. Directs the education of CDI employees about their security and privacy protection responsibilities. Develops and implements plans to streamline and improve policies, procedures, standards, and guidelines, which will enhance CDI's overall security position. Collaborates with CDI's executives and senior managers to integrate administrative security controls into business processes and procedures. Conducts

**ESSENTIAL FUNCTIONS DUTY STATEMENT**HRM-025

---

maturity assessments to identify gaps and develop alternatives for investment recommendations to improve Department security posture. This work may involve comparing baseline information in certain subject areas such as technology, system users, or Information Technology (IT) processes, against control agency requirements as issued by information security oversight organizations such as California Department of Technology (CDT) and National Institute of Standards and Technology (NIST).

- 25%** Provides direct supervision, leadership, and policy direction to the Information Security staff responsible for risk identification, threat detection, analysis, investigation, incident response, security monitoring, security consulting, and vulnerability assessments. Organizes, prioritizes, and directs staff workload. Develops annual goals, and objectives as well as workload and performance measures. Oversees the activities of information security staff; establish priorities for staff and vendors assigned to team efforts; establishes work standards and measurements for the team; reviews work for completeness, accuracy, schedule conflicts, and fulfillment of requirements. Performs employee evaluations, completes probation reports and annual appraisals; responsible for staff training and development; responsible for managing issues and risks, and reporting program status to management and customers. Conducts recurring "one on one" meetings with direct reports.
- 20%** Consults with and advises peers in the IT Division, CDI's Privacy Officer, and the lines of business to continuously improve processes to secure the confidentiality, integrity, availability of member data and information. Serves as the information security expert in CDI governance councils and organization-wide forums. Advises and consults on matters related to business continuity and the mitigation of business disruption. Participates in Enterprise Risk Management meetings as needed. Develops physical security criteria and checklists.
- 15%** Researches and evaluates current and new information security technology and trends which, in collaboration with ITD, ensures information security requirements are addressed in developing a Departmental and Department information security architecture roadmap. Collaborates with the State of California's Information Security Officer (ISO) and the CDI's Chief Information Officer (CIO) to ensure alignment with statewide information security initiatives; leads and participates in security planning sessions.

**MARGINAL FUNCTIONS**

- 5%** 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 and submits time into the appropriate time accounting system by the due date.

---

**WORK ENVIRONMENT OR PHYSICAL ABILITIES**

Work Environment:

- Must be able to work in a high-rise building.
- Prolonged periods of standing, bending or sitting.
- Work hours may vary, such as work shift, weekends, evenings and/or holidays.

**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 Health & Safety Analyst.)

\_\_\_\_\_  
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