State of California
Business, Consumer Services and Housing Agency
California Department of Housing and Community Development
DUTY STATEMENT

Division:	Administration and Management
Unit:	Information Technology Branch
Position Number:	401-111-1405-004 (PS 2622)
Classification:	Information Technology Manager I
Working Title:	Chief Information Security Officer
Location:	Sacramento Headquarters
Incumbent:	Vacant
Effective Date:	TBD

Department Statement: You are a valued member of the Department's team. You are expected to work cooperatively with team members and others to enable the Department to provide the highest level of service possible. Your creativity and ingenuity are encouraged. Your efforts to maintain regular attendance and treat others fairly, honestly, and with respect are critical to the success of the Department's mission.

Job Summary: Under general direction of the Chief Information Officer (CIO), the Information Technology Manager I (ITM I) serves as the Chief Information Security Officer (CISO) for the Department of Housing and Community Development (HCD). The CISO has full management responsibility for the Information Security Office and provides leadership, supervision, guidance, mentoring, and support for all activities associated with the Department's information security program. The incumbent is responsible for implementing information security policies, standards, guidelines, processes, and procedures to safeguard the confidentiality, integrity, and availability of HCD's systems, applications, data, interfaces, and information processing infrastructure. This position will provide services from IT domains of Information Security Engineering, System Engineering, and Information Technology Project Management.

% of Time **Essential Functions:**

30% Information Security Strategic Planning and Policy Management

Under the general direction of the CIO, formulate the information security program objectives and develop the department's information security strategy and roadmap. Develop, implement, and maintain information security policies, standards, guidelines, processes, and procedures in accordance with the department's strategy, State Office of Information Security (OIS) policies and guidance, and other applicable state and federal regulations. Ensure that the security policies and procedures are reviewed and updated as needed to prevent new threats and vulnerabilities. Direct the maintenance and enforcement of security policies and standards to safeguard HCD's information, information systems, information processing infrastructure and interfaces with effective security controls. Serve as the information security point of contact for external agencies including OIS on all information security matters. Establish cooperative relationships with management, data owners, data custodians, and information users. Conduct analysis and prepare reports related to information security trends and best practices to be continuously prepared for improving the Department's security posture, utilizing inputs from staff, customers, peers, and independent research.

30% Information Security Program and Risk Management
Provide leadership, supervision, guidance, mentoring, and support for all activities associated with the Department's information security program. Conduct information security and risk assessments and monitoring activities to identify vulnerabilities, threats, and risks within the department's information resources and data custodian environments. Coordinate independent security assessments and audits. Make recommendations, direct the development of effective and economical solutions, plan actions and milestones, and oversee their implementation to address assessment and audit findings. Direct and coordinate the information classification processes and business impact assessments for technology recovery and business continuity planning. Coordinate the preparation and testing of disaster recovery and business continuity processes. 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. Ensure department staff are educated on information security and privacy protection responsibilities and are following the policies to appropriately use department's information resources. Develop and implement appropriate procedures to manage security incidents. Act as the incident manager for any security incidents, direct investigative activities, recommend corrective action plans, and coordinate their implementation. Provide required reports to control agencies on the implementation of HCD's information security program and ongoing compliance with the State's security and risk management policies.

20% Security Technology Operations
Direct and manage the design, development, implementation, and ongoing support of information security technologies including the Boundary Protection, Threat and Vulnerability Management (TVM), Security Information and Event Management (SIEM), and Privileged Access Management (PAM) solution components. Collaborate with the Infrastructure and Platform Services teams to implement and operate industry-strength tools and technologies for endpoint protection, perimeter defense, malware defense, intrusion prevention, network segmentation, and other preventative controls. Collaborate with department's infrastructure and application development teams to manage the design and implementation of information security technical controls and/or threat countermeasures. Manage Information Security Governance to ensure alignment of information security objectives with the business strategy, optimized security investments and measurable results.

10% Personnel Management

Create and maintaina team of talented IT professionals and foster an environment of trust and success, where highly qualified and high-performing staff are retained. Establish performance standards and expectations to staff and offer clarity, guidance, sound judgement, and discretion to positively influence staff in achieving successful outcomes. Establish and uphold a culture of customer service to internal and external stakeholders. Manage the administrative processes (vacation, sick leave, overtime, timesheets, and travel authorization) to ensure sufficient coverage and support. Ensure staff has appropriate training and skills necessary to effectively perform tasks and carryout responsibilities.

5% Planning and Administration

Participate in the development and management of short and long-range plans encompassing both strategic and operational needs including budget and staffing plans. Prepare, negotiate, and present ISO budget and other funding proposals. Monitor expenditures and operate within budget allocation. Ensure that ISO meets all administrative and IT mandates, departmental and statewide policies and procedures, and control agency guidelines.

% of Time **Marginal Functions:**

5% Meet as appropriate with other ITB managers and the CIO to share information. Conduct periodic meetings to keep staff apprised of office, branch, and departmental updates. Perform other related duties, as assigned, to ensure efficient and effective achievement of organization’s goals and objectives. Perform other duties as assigned.

Special Requirements: (Define all that apply)

Travel: Up to 5% overnight travel throughout the state may be required.

Supervision Exercised: The incumbent directly supervises a variety of IT professionals IT Specialist I to IT Specialist II classifications. The incumbent may also manage vendors in their performance of work activities associated with the ISO. The incumbent may also collaborate with multi-disciplinary teams drawn from within other IT sections to ensure success of the information technology projects.

Conflict of Interest (COI): Form 700 reporting required

Background Check: None

Live Scan: None

Bilingual, specify language: None

License/Certification: None

Medical Clearance: None

Other, please specify: This position requires strong organizational, technical, written and management skills and an aptitude toward learning and applying technical knowledge. Since the incumbent will be in frequent contact with users, he/she should possess excellent interpersonal communication skills.

Physical Requirements: The position requires the ability to sit, stand, read, communicate, and work on a computer for extended periods of time.

Working Conditions (In Office): The incumbent works in an office setting in an air conditioned, high-rise building with elevator access, cubicle, or office with natural and artificial lighting.

Working Conditions (Telework): The incumbent is required to maintain safe working conditions at the approved alternate work location and abide by the Department's Ergonomic Program guidelines and agrees to maintain a distraction-free remote work environment.

Administrative Responsibility: The ITM I is responsible for all management functions of the ISO, including performance appraisals, hiring, etc. Additionally, the incumbent has contract management responsibility for all contracts associated with the ISO.

Personal Contacts: The incumbent will have daily and frequent contact with all levels of Department management and vendors and contract staff. Additionally, the incumbent will participate in interdepartmental user groups.

Consequence of Action: The ITM I will function with a high degree of independence and is required to have accurate prioritization skills, excellent organizational skills, excellent communication, and problem assessment and resolution skills. The ITM I must be aware of, and able to properly apply, all applicable state rules, regulations, laws, processes, and procedures to each functional area of responsibility. Poor decision making or failure to make correct recommendations would adversely impact the delivery of IT projects and initiatives. Consequence of error may have statewide and enterprise-wide impacts including lost funding, project failure, poor customer service, risk exposure, loss of business continuity, and budget implications.

Diversity, Equity and Inclusion: All employees at HCD are expected to uphold the values of diversity, equity and inclusion (DEI) which includes being committed to fostering an environment in which employees from a variety of backgrounds, cultures, and personal experiences feel welcomed and can thrive. Staff are expected to be respectful of differences, treat others with respect, encourage others to participate, foster innovations, and stay committed to all DEI efforts in the workplace.

Equal Employment Opportunity: All HCD employees are expected to conduct themselves in a professional manner that demonstrates respect for all employees and others they meet during work hours, during work-related activities, and anytime they represent the Department. Additionally, all HCD employees are responsible for promoting a safe and secure work environment, free from discrimination, harassment, inappropriate conduct, or retaliation.

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.)

Employee Name: ______________________________ Date: _____________

Employee Signature: ______________________________

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.

Supervisor Name: ______________________________ Date: ___________

Supervisor Signature: ______________________________

*Please return the signed original duty statement to the Human Resources Branch to be filed in the Official Personnel File.