Employment Development Department
State of California

☒ Current
☐ Proposed

POSITION STATEMENT

1. POSITION INFORMATION

Civil Service Classification Information Technology Manager II	Working Title Privacy and Integrated Risk Management Office Manager
Name of Incumbent	Position Number 280-390-1406-001
Section/Unit Privacy and Integrated Risk Management Office	Supervisor's Name
Division Cybersecurity Division	Supervisor's Classification CEA B
Branch Information Technology	Duties Based on: ☒ Full Time ☐ Part Time - Fraction
	Revision Date 5/21/2023

2. REQUIREMENTS OF POSITION

Check all that apply:

☒ Conflict of Interest Filing (Form 700) Required	☐ Call Center/Counter Environment
☐ May be Required to Work in Multiple Locations	☒ Requires Fingerprinting & Background Check
☐ Requires DMV Pull Notice	☐ Bilingual Fluency *(specify below in Description)*
☒ Travel May be Required	☐ Other *(specify below in Description)*

Description of Position Requirements *(e.g., qualified Veteran, Class C driver's license, bilingual, frequent travel, graveyard/swing shift, etc.)*

3. DUTIES AND RESPONSIBILITIES OF POSITION

Information Technology Domains

☒ Business Technology Management	☐ IT Project Management	☐ Client Services
☒ Information Security Engineering	☐ Software Engineering	☐ System Engineering

Under the administrative direction of the Employment Development Department (EDD) Cybersecurity Division Chief, the Information Technology Manager (ITM) II is designated as the Privacy and Integrated Risk Management Office. The Privacy and Integrated Risk Management office provides governance and direction risk management program, privacy program, and incident response program.

The Privacy and Integrated Risk Management Office has a significant breadth and depth of understanding of the EDD's business process needs, assesses internal and external risks, provides appropriate mitigation strategies, and stays current on relevant laws and regulations. Privacy and Integrated Risk Management Office keeps abreast of technologies to ensure the appropriate risk mitigation plans are developed and prioritized in coordination with Information Technology Branch.

Additionally, the Privacy and Integrated Risk Management Office provides management and direction for the Department's Privacy Officer and is responsible for overseeing the Privacy policies and programs.

The Privacy and Integrated Risk Management Office role has four types of activities:

- Planning – Determines an annual work plan to achieve security goals and objectives consistent with the Department's strategic plan.
- Developing – Oversees the development of risk management program, standards, guidelines, processes, and procedures.
- Managing – Through subordinate staff, conducts risk assessments, manages incidents, provides internal and external reporting and maintains the Department's security awareness education and training.
- Oversight – Evaluates the effectiveness of ongoing risk management program, privacy program and incident response program for effectiveness in establishing corrective action plans, risk mitigation plans, or privacy controls in alignment with internal and external requirements (e.g., laws, regulations, statutes, state policy, etc.)

The Privacy and Integrated Risk Management Office contributes toward the growth of the IT Branch into a customer-focused service organization by developing and implementing policies and procedures for progressive information solutions and by providing constructive feedback to others within the Branch.

3. DUTIES AND RESPONSIBILITIES OF POSITION *(continued)*

Percentage of Duties	Essential Functions
40%	Administers the Department's risk management program by developing risk management policy, establishing strategic goals and long-range objectives, and determining new enterprise-wide risk mitigation plan and policy decisions. The Privacy and Integrated Risk Management Office plans, organizes, and directs, through subordinate managers and supervisors, the following risk management activities: • Direct and oversees the risk management program, continuous risk assessment of critical business processes and associated information systems, and the development and prioritization of risk mitigation plans in alignment with department goals and objectives. • Establishes in coordination with departmental executives risk tolerance and the risk acceptance process in association for managing information security and privacy risk. • Evaluates business requirements and security architecture for departmental projects to ensure information security and privacy controls are established in the design phase and tested and evaluated for effectiveness. • Manages risk assessments to identify potential vulnerabilities that could threaten the security of the Department's information assets. Determines the probable loss or consequences of identified threats and assesses the likelihood of such occurrences
25%	Administers the department's privacy program by developing privacy policy, establishing strategic goals to mitigate privacy risk and determining new and enterprise-wide privacy objectives. The Privacy and Integrated Risk Management Office plans, organizes and directs, through subordinate managers and superivsiors the following privacy management activities: • Directs and oversees the privacy program, the continuous privacy threshold analysis and privacy impact assessments of departmental business processes, projects and programs and the development and prioritization of privacy risk mitigation plans in alignment with department goals and objectives. • Evaluates privacy risk associated with contracts, and data sharing agreements and communicate with the Cybersecurity Division Chief and executives and the risk associated and the strategic alternatives. • Ensures requests for release of personal/confidential information are correctly evaluated and authorized or denied based on existing laws, regulations, and polices. • Oversees development and administration of reimbursable confidential information disclosure contracts with local, state, and federal agencies entitled to Department information. Administers onsite reviews of entities receiving Department information to ensure those entities are maintaining appropriate safeguards to protect Department data and are complying with the confidentiality requirements of their contracts.
20%	Oversees development and reviews implementation of policies and procedures for reporting incidents involving intentional, unintentional or unauthorized use, modification,

	access, or destruction of the Department's information assets. Coordinates with and assists the Investigation Division during investigations of alleged incidents of security violations.. Reports security incidents to executives, control agencies, and law enforcement. Collaborates with branches post-incident reviews, develops action plans to reduce further exposure, and evaluates and reports on trends and weaknesses in EDD's security program.
10%	Develops staff and carries out Department and Branch succession plan strategies. Completes training plans, probation reports, and other personnel-related products in a timely manner, according to the EDD Personnel Management Handbook. Manages administrative activities for group staffing and budgeting. Plan group's workload and maintains staff time estimates for projects and line of business activities. Prepares and provides weekly status report, and reviews the status reports of suborindate managers. The incumbent demonstrates knowledge on laws, rules, regulations, and polices including, but not limited to, Government Code, Public Contracting Code, State Administrative Manual, Statewide Information Management Manual, and the State Contracting Manual, which are relevant and applicable to their lines of business.

.

Percentage of Duties	Essential Functions
5%	Performs other duties as assigned.

4. WORK ENVIRONMENT *(Choose all that apply from the drop-down menus)*

Standing:	Intermittent (34-50%)	Sitting:	Intermittent (34-50%)
Walking:	Intermittent (34-50%)	Temperature: Environment	Temperature Controlled Office
Lighting:	Artifical Lighting	Pushing/Pulling:	Not Applicable
Lifting:	1-25% of the time	Bending/Stooping:	Not Applicable
Other:			

Type of Environment: a. Cubicle b. N/A c. N/A d. N/A

Interaction with Public: a. N/A b. N/A c. N/A.

5. SUPERVISION

Supervision Exercised *(e.g., Directly – 1 Staff Services Manager I; Indirectly – 5 SSAs / AGPAs)*

Directly – (1) ITM I; (1) Staff Services Manager I ;
Indirectly – (1) IT Supervisor II; (2) IT Specialist II; (3) IT Specialist I; (1) IT Associate; (3) AGPA; (1) SSA

6. SIGNATURES

Employee's Statement:
I have reviewed and discussed the duties and responsibilities of this position with my supervisor and have received a copy of the Position Statement.

Employee's Name (Print)

Civil Service Classification
Information Technology Manager II

Position Number
280-390-1406-001

Employee's Signature

Date

Supervisor's Statement:
I have reviewed the duties and responsibilities of this position and have provided a copy of the Position Statement to the Employee.

Supervisor's Name (Print)

Supervisor's Signature

Date

7. HRSD USE ONLY

Personnel Management Group (PMG) Approval

☒ Duties meet class specification and allocation guidelines.

PMG Analyst initials: dmg

Date approved: 7/13/2023

Reasonable Accommodation Unit use ONLY *(completed after appointment, if needed)*

* If a Reasonable Accommodation is necessary, please complete a Request for Reasonable Accommodation (DE 8421) form and submit to Human Resource Services Division (HRSD), Reasonable Accommodation Coordinator.

List any Reasonable Accommodations Made:

**** AFTER SIGNATURES ARE OBTAINED:**

- **SEND A COPY OF POSITION STATEMENT TO HRSD (VIA YOUR ATTENDANCE CLERK) TO FILE IN THE EMPLOYEE'S OFFICIAL PERSONNEL FILE (OPF)**
- **FILE ORIGINAL IN THE SUPERVISOR'S DROP FILE**
- **PROVIDE A COPY TO THE EMPLOYEE**