Employment Development Department
State of California

☐ Current
☒ Proposed

POSITION STATEMENT

1. POSITION INFORMATION	
CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Manager I	Cybersecurity Risk Manager
NAME OF INCUMBENT:	POSITION NUMBER:
	280-390-1405-013
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Information Security Office/Risk Management	
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Information Security Office	Information Technology Manager II
BRANCH:	REVISION DATE:
Information Technology Branch	10/15/2021

Duties Based on: ☒ FT ☐ PT– Fraction _____ ☐ INT ☐ Temporary – _____ hours

2. REQUIREMENTS OF POSITION

Check all that apply:

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

May be required to move certain equipment.

3. DUTIES AND RESPONSIBILITIES OF POSITION

Summary Statement:
(Briefly describe the position's organizational setting and major functions)

Information Technology Domains (Select all domains applicable to the incumbent's duties/tasks.)

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

Under the general direction of the Information Technology (IT) Manager II, the Information Technology Manager I has significant responsibilities for formulating or administering cybersecurity measures for risk management. The incumbent serves as a subject matter expert (SME) of the California Cybersecurity Maturity Metrics, as defined by SIMM 5300-C, to ensure EDD alignment with the five security domains (Identify, Protect, Detect, Respond, and Recover). The IT Manager I will ensure that risk assessments, vulnerability assessments, and threat analysis are conducted constantly, and at appropriate times to identify and assess risk to EDDs data. The IT Manager I will oversee staff and provide leadership to ensure that the EDD Information Security and Privacy Policies are in alignment with the State Administrative Manual (SAM) Section 5300 and the Statewide Information Management Manual, Information Security Program

Management Standard (SIMM 5305-A). The incumbent serves as a security Architect in support of the organization's enterprise information technology operations, including all associated hardware/software components and the confidential and sensitive data used at EDD.

The incumbent advises and assists the EDD and Labor and Workforce Development Agency (LWDA) Information Security Officer, the EDD / LWDA Privacy Coordinator and the EDD Technology Recovery Coordinator and will serve as the designated backup for the EDD Information Security Officer and the EDD Privacy Coordinator.

Responsibilities include a full range of management support activities, including, but not limited to: planning the group's training, hardware and software needs and budget; building staff capacity; planning future projects and directing current projects; assigning resources; completing special studies; managing consultants hired to augment State staff; and completing required personnel activities.

The incumbent contributes toward the growth of the Information Technology Branch (ITB) into a customer-focused service organization by developing and implementing policies and procedures for progressive information solutions and by providing feedback to others within the Branch.

Percentage of Duties	Essential Functions
45%	Provides leadership and direction to the Risk Management staff, overseeing the development, improvement, maintenance, and support of ISO processes and policies. Performs high level technical and managerial tasks as a security architect in support of the Information Security Office's (ISO) lines of business. Provides guidance to project managers and programs on the completion of the business impact analysis, privacy impact assessments/threshold and Information System Recovery Plan/Technology Recovery Plan documents ensuring all are completed through project implementation. Provides guidance on the System Security Plan (SSP) development and review. Serves as manager and primary contract monitor for the ISO. Performs contract management duties, including coordinating amendments, tracking contractor activities and managing the invoicing process. Ensures all mandated state and federal reporting requirements are completed within the specified timeframes. Serves as manager and technical architect over risk management tasks ensuring compliance with the California State Adminstrative Manual (SAM), Statewide Information Management Manual (SIMM), Internal Revenue Service (IRS) Publication 1075 and security industry standards (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), etc. Directs the documentation for security risk assessments, ensuring timely updates are provided to project stakeholders, system owners, and Internal/Federal/State auditors. Oversee staff working with system owners to ensure all EDD security plans, standards and procedures, following security best pactices adhering ot risk management frameworks under NIST. Formulates, analyzes, and makes recommendations on the impact of legislation to the Department's information security assets and plans for its implementation under the direction of State, Departmental and other applicable government policies and regulations. Oversees the development and execution of certification and accreditation documentation which is presented to the EDD executive management.
25%	Performs Managerial level technical review and analysis of all IT security policies and standards, annually reviews all IT security policies, standards, forms, plans, training and information security directives and oversees clearance of all ISO-related publications. Ensures information systems are compliant with all department, state, and federal information technology and security requirements. Performs as the Departments's backup Information Security Officer and Labor Work Development Agency backup Agency Information Security Officer.

	Ensures timely Security Advisories and Alerts are sent, specifically to the Systems Administrators and the IT Customer Service Group for all of the EDD. Leads the ISO staff, Central IT (CIT) and Distributed IT Systems Administrators with high level security technical advice and assistance. Routinely manages and directs the analysis of Applications Security and Website Compromise security incidents and the actions associated with security hardening, protections and mitigation. Reviews and monitors security alerts and patches related to software vendors. Oversees the informal and formal security reviews and assessments of both CIT and DTS related applications environments.
15%	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. Plans group's workload and maintains staff time estimates for projects and line of business activities. Prepares and provides weekly status report. 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	**Marginal Functions**
10%	Oversees the participation of the risk management group in confidential investigations, including log and audit reviews, email pulls, end point forensics, and other forensic activities, regarding use of EDD information assets consistent with the EDD Electronic Access Standard.
5%	Performs other duties as assigned.

4. WORK ENVIRONMENT *(Choose all that apply)*

Standing: Occasionally - activity occurs < 33%	Sitting: Frequently - activity occurs 33% to 66%
Walking: Occasionally - activity occurs < 33%	Temperature: Temperature Controlled Office Environment
Lighting: Artificial Lighting	Pushing/Pulling: Occasionally - activity occurs < 33%
Lifting: Occasionally - activity occurs < 33%	Bending/Stooping: Occasionally - activity occurs < 33%

Other: *Click here to enter text.*

Type of Environment:
☒ High Rise ☒ Cubicle ☐ Warehouse ☐ Outdoors ☒ Other**:** Telework

Interaction with Customers:
☐ Required to work in the lobby ☐ Required to work at a public counter
☐ Required to assist customers on the phone ☐ Required to assist customers in person
☐ Other:

5. SUPERVISION EXERCISED:
(List total per each classification of staff)

Directly- 1 IT Supervisor II; 2 IT Specialist II. Indirectly - 5 IT Specialist I; 1 IT Associate.

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:

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:

Supervisor's Signature: Date:

7. HRSD USE ONLY

Personnel Management Group (PMG) Approval

☒ Duties meet class specification and allocation guidelines. ☐ Exceptional allocation, STD-625 on file.	PMG Analyst Initials dmg	Date Approved 10/15/2021

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:

Supervisor: After signatures are obtained, make 2 copies:

- Send a copy to HRSD (via your Attendance Clerk) to file in the employee's Official Personnel File (OPF)
- Provide a copy to the employee
- File original in the supervisor's drop file