Employment Development Department
State of California

☐ Current
☒ Proposed

POSITION STATEMENT

1. POSITION INFORMATION	
CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
IT MANAGER II	Cybersecurity Operations Office Manager
NAME OF INCUMBENT:	POSITION NUMBER:
	390-1406-002
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Cybersecurity Operations Office	*Click here to enter text.*
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division	CEA B
BRANCH:	REVISION DATE:
Information Technology Branch	

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.)

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 administrative direction of the CEA B, Cybersecurity Division Chief, the Information Technology (IT) Manager II oversees the Cybersecurity Operations Office. Work performed is primarily in the Information Security Engineering Domain. The IT Manager II develops and maintains information security related policies and procedures for EDD that incorporate applicable federal, state, local, and industry legal, statutory, and regulatory requirements. Ensures ongoing integrated risk management monitoring and assessment review processes are in-place to identify and report upon potential breeches or non-compliance. Plans for and

utilizes Data Discovery and Classification Tools to ensure data moving from system to system or through cloud services have correct classification and the ability to ensure only appropriate and authorized data is allowed in these systems. Ensures implementation and maintenance of cybersecurity and fraud detection solutions and countermeasures, and continuously monitors for reporting of issues or problems for management review. Ensures implementation of appropriate information/data and systems vulnerabilities privacy protection processes and appropriate disclosure and fraud practices are in-place to ensure that personally identifiable information, e.g., personal and federal income tax information (FTI) is protected with operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability, and to prevent unauthorized or inappropriate access, use, or disclosure.

Percentage of Duties	Essential Functions
35%	Directly manages an IT Specialist III in the development of an EDD enterprise-wide Fraud Protection Architecture. In addition, through two subordinate IT Managers, manages office staff in design, testing, implementation and maintenance of policies and procedures to: safeguard the security of EDD's Information Technology operations; deploy robust vulnerability detection monitoring; support secure Cloud-based operations; and develop and deploy cybersecurity countermeasures to assess and test EDD's IT applications and systems for potential weakness that could be exploited. Manages a Cybersecurity Operation and Fraud Center to constantly monitor on a 24x7 basis the ever-evolving cyber-attacks and benefit fraud tactics that are being utilized by individuals, organized criminals, and foreign nation states; identify solutions for fraud mitigation and improve cybersecurity and suspicious event monitoring, response, and resiliency. Ensures collaboration with program areas and the IT Branch in monitoring and maintenance of Business Resumption and Disaster Recovery policies and procedures for resumption of all operations in the event of cybersecurity breeches. Makes timely reports to the Cybersecurity Division Chief regarding cybersecurity and fraud related issues, and remedial mitigation actions taken.
25%	Oversees staff in secure cybersecurity, enhancements, suspicious activity monitoring tools, and training as necessary to proactively address vulnerabilities, threats and security findings, implement technology to mitigate benefit fraud, meet the increasing need in cyber risk management, and strengthen the EDD cybersecurity posture. Builds long-term, sustainable, and flexible processes that will allow EDD to serve the people of California securely. Manages staff in development and implementation of IT systems security plans and procedures and security software tools, e.g., Application Security Assessment Tools**.** Develops and implements a system security test and evaluation plan in compliance with SAM 5315.4. Ensures ongoing staff training to keep abreast of developing Information Technology Privacy requirements and safeguards, legal issues related to privacy projects, protections for personal and federal income tax information (FTI), legal considerations and requirements for information disclosure including privacy and breeches, and emerging IRM best practices.
25%	Manages vendor contracts to ensure statements of work or services are properly being performed. Manages the planning and production required security auditing obligations and reports, e.g., IRS PUBLICATION 1075, to perform monthly vulnerability assessments of EDD's applications due to their interaction with Federal Taxpayer Information (FTI). Ensures policy creation, procedure development, implementation and maintenance for cybersecurity; fraud detection, prevention, and mitigation; vulnerabilities detection, prevention, and mitigation; securing Cloud service providers; and application and systems security testing. Formulates, analyzes, and makes recommendations on the impact of legislation and plans for its implementation under the direction of State, Departmental and other applicable government policies and regulations. Facilitates IT strategic planning sessions and workshops. Works with control agencies to comply with state administrative requirements.

Percentage of Duties	**Marginal Functions**
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. Plans group's workload and maintains staff time estimates for projects and line of business activities. Prepares and provides weekly status report.
5%	Other duties as assigned

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

Standing: *Choose an item.*	Sitting: *Choose an item.*
Walking: *Choose an item.*	Temperature: *Choose an item.*
Lighting: *Choose an item.*	Pushing/Pulling: *Choose an item.*
Lifting: *Choose an item.*	Bending/Stooping: *Choose an item.*
Other:	

Type of Environment:

☐ High Rise ☐ Cubicle ☐ Warehouse ☐ Outdoors ☐ Other**:**

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)

1 – IT Specialist III; 2 IT Manager I

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.	PMG Analyst Initials	Date Approved

☐ Exceptional allocation, STD-625 on file.		

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