Employment Development Department
State of California

☐ Current
☒ Proposed

POSITION STATEMENT

1. POSITION INFORMATION	
CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Manager I	Cybersecurity Operation & Fraud Center Manager
NAME OF INCUMBENT:	POSITION NUMBER:
	390-1405-005
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Cybersecurity Operations Office / Cybersecurity Operation & Fraud Center	*Click here to enter text.*
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division	Information Technology Manager II
BRANCH:	REVISION DATE:
Information Technology Branch	11/20/2022

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 the general direction of the Information Technology (IT) Manager II over the Cybersecurity Operations Office, the IT Manager I directs and manages staff in the Cybersecurity Operation & Fraud Center of the Employment Development Department's (EDD) Information Technology Branch (ITB). The Cybersecurity Operation & Fraud Center protects EDD against cyber threats.

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 incumbent also contributes toward the growth of the 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.

Responsibilities include a full range of unit 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.

Percentage of Duties	Essential Functions
30%	Manages, plans, develops, and documents security testing and assessment policies, requirements, methodologies, frequencies, and work activities of the Cybersecurity Operation & Fraud Center. Oversees staffs' round-the-clock monitoring of EDD's network and the identification of any potential cyber-attack or intrusion (event) and determines if it is a genuine malicious threat (incident), and if it could affect business. Executes timely review of security-related intelligence if possible/actual cyberattack is detected and takes steps necessary to remediate it. Manages and provides timely Security Advisories and Alerts, specifically to the Systems Administrators and the EDDNext Steering Committee Section when necessary to elevate awareness. Reviews, performs, and provides technical reviews, advisory communication, and coordination regarding Microsoft (and other software vendors') Cybersecurity announcements and software security patch releases. Oversees and performs informal and formal security reviews and assessments of both Central IT (CIT) and Distributed IT (DIT) related applications environments.
30%	Oversees a persistent focus on providing policies, creating procedures, and monitoring activities to situational awareness through the detection, containment, and remediation of IT threats in order to manage and enhance an organization's security posture. Manages any threatening IT incidents, and ensures they are properly identified, analyzed, communicated, investigated and reported. Sets cybersecurity goals and objectives to ensure employees and all authorized users of EDD systems and applications understand and guard against fraudulent activities such as phishing, social media engineering, viruses, and denial of service attacks. Collaborates and consults with IT and Non-IT lines of business on IT projects and serves as a subject matter vulnerability expert in state and federal security and privacy laws, regulations, and policies. Coordinates and or collaborates in internal and external security audits. Provides analytical, technical reviews to ensure all IT Cybersecurity and Fraud security policies and standards are adhered to. Ensures information systems are compliant with all Departmental, state, and federal IT and security vulnerability requirements.
25%	Manages and conducts annual reviews of Cybersecurity and Fraud protection Security standards, the Information Security and Privacy Policy (ISPP), Cybersecurity Charter and other Information Security Directives. Oversees and provides timely updates on system security plans (SSPs) with the plan/system owner(s), coordinates rules of engagement discussions for application security vulnerability assessments/penetration testing, develops the system plan of action and milestones, and facilitates the certification and accreditation documentation which is presented to the EDD executive management. Ensures compliance with all applicable state and federal regulatory requirements to protect sensitive data and complies with industry best cybersecurity and fraud awareness identification and protection practices and standards. Supervises, coordinates and participates in confidential investigations and audits, 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. Manages vendor support contracts including software, hardware and services contracts.

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. 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.
5%	Performs other duties as assigned.

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

Standing: Occasionally - activity occurs < 33%	Sitting: Continuously - activity occurs > 66%
Walking: Occasionally - activity occurs < 33%	Temperature: Temperature Controlled Office Environment
Lighting: Artificial Lighting	Pushing/Pulling: Not Applicable - activity does not exist
Lifting: Not Applicable - activity does not exist	Bending/Stooping: Not Applicable - activity does not exist

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)

Directly – 3 IT Specialist II; 4 IT Specialist 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. ☐ Exceptional allocation, STD-625 on file.	PMG Analyst Initials dmg	Date Approved 1/3/2023

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:

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