EDD Employment Development Department
State of California

☐ Current
☒ Proposed

POSITION STATEMENT

1. POSITION INFORMATION

CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Manager I	Vulnerability Group Manager
NAME OF INCUMBENT:	POSITION NUMBER:
	390-1405-007
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Cybersecurity Operations Office / Vulnerability Group	Information Technology Manager II
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Services Division	Information Technology Manager II
BRANCH:	REVISION DATE:
Information Technology Branch	11/19/2022

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
☒ Information Security Engineering
☒ IT Project Management
☒ Software Engineering
☐ Client Services
☒ 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 Vulnerability Group within the Cybersecurity Division. Collaborates on the use of new software tools EDD will use to perform comprehensive security reviews of millions of lines of code residing in applications used to process benefits. Tools will include Application Security Assessment, Integrated Risk Management (IRM), Governance Risk and Compliance (GRC), and Data Discovery and Classification. Code reviews resulting from use of these tools will be used to identify and remediate potential exploitation points and system vulnerabilities, which are ever evolving threats cybercriminals can use to commit benefit theft and fraud. The incumbent 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

Percentage of Duties	Essential Functions
30%	Manages, plans, and directs work activities of the Vulnerability Group including developing, and documenting security testing and assessment policies, requirements, methodologies, and frequencies. The work performed by the specialists includes: creating, reviewing, and updating EDD’s information security vulnerability standards, policies and guidelines, including dissemination; analyzing EDD’s cyber defense policies and configurations, and evaluating compliance with regulations and organizational directives; conducting and supporting authorized penetration testing on enterprise network assets; maintaining a deployable cyber defense audit toolkit with specialized cyber defense software and hardware to support cyber defense audit missions; maintaining current knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing; preparing audit reports that identify technical and procedural findings, and providing recommended remediation strategies and solutions; conducting Technical Surveillance and Countermeasure Reviews as appropriate within environment; performing risk and vulnerability assessments of technology, people, and operations across relevant technology focus areas - local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications; developing recommendations for the selection of cost-effective security controls to mitigate risk; categorizing identified vulnerabilities based on severity, impact and class of vulnerability in order to prioritize remediation including a strategy for addressing the vulnerabilities; developing, implementing and maintaining Application security policies and procedures that introduce a secure software development life cycle for development teams to safeguard, find, fix and preferably prevent vulnerability and security issues within applications.
30%	Manages high-level vulnerability security tasks for the Vulnerability Group. Develops and maintains compliance and IT Vulnerability Security policies, standards, and procedures using the California State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), Internal Revenue Service (IRS) and security industry standards - International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST). Provides oversight to staff in working with system owners to develop and maintain System Security Plans (SSPs). Ensures EDD staff observe vulnerability standards and produce quality work products that follow security best practices adhering to frameworks under NIST IRS Publication 1075. Manages and conducts annual reviews of Vulnerability Security standards, the Information Security and Privacy Policy (ISPP), Cybersecurity Charter, and other Information Security directives. Oversees and provides timely updates on SSPs with the appropriate owner(s), coordinates rules of engagement discussions for application security vulnerability assessments and penetration testing, develops the system plan of action and milestones, and facilitates the certification and accreditation

	documentation presented to EDD executive management. Provides analytical and technical reviews to ensure all IT Vulnerability 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 provides timely Security Advisories and Alerts for the Systems Administrators and the IT Customer Service Section when needed. Provides security technical advice and assistance in support of the Cybersecurity staff, Central IT (CIT) and Distributed IT (DIT) Systems Administrators as required. Troubleshoots and refers actions associated with security hardening, protections, and mitigation. Performs, evaluates, and provides technical reviews, advisory communications, and coordination of Microsoft (and other software vendors) Security announcements and software security patch releases. Oversees and performs informal and formal security reviews and assessments of both CIT and DTS related applications environments. Reviews and disseminates security related intelligence. Supervises, coordinates, and participates in confidential audit and 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. 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. Manages vendor support contracts including software, hardware and services contracts to ensure statements of work or services are properly being performed.
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; 3 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	Date Approved
	dmg	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