EDD Employment Development Department
State of California

☐ Current
☒ Proposed

POSITION STATEMENT

1. POSITION INFORMATION

CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Specialist III	Cybersecurity & Fraud Architect
NAME OF INCUMBENT:	POSITION NUMBER:
	280-390-1405-001
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Cybersecurity Operations Office	*Click here to enter text.*
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division (CSD)	Information Technology Manager II
BRANCH:	REVISION DATE:
Infromation Technology Branch	7/6/2023

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.)

Click here to enter text.

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
X Information Security Engineering
X IT Project Management
X Software Engineering
☐ Client Services
X System Engineering

Under the administrative direction of the Cybersecurity Operations Office Manager (Information Technology Manager II), the Information Technology Specialist III (ITS III) serves as the Cybersecurity Architect and expert advisor in concepts and theories of fraud detection and mitigation. Follows administrative direction from the Cybersecurity Operations Office Manager with a high degree of independence and expertise. The Cybersecurity & Fraud Architect has an advanced enterprise-wide level of understanding of EDD's information technology (IT) architecture. Applies a master level of technical IT expertise to connect strategic intent and practical technical application in the development of a full range of fraud threat reduction, vulnerability reduction, deterrence, incident response, resiliency, recovery policies, fraud detection standards, analytics and concepts governing methods for data storage to support fraud detection. Collaborates with ITB Divisions and business units in the planning, designing, testing and implementing a fraud threat detection and mitigation architecture. Develops prerequisites for networks, firewalls, routers, and other network devices. Performs vulnerability and fraud assessments, security testing, and risk analysis. Continuously researches and implements updated fraud security standards and best practices in compliance with applicable state and federal laws, rules and regulations. Recognizes the criticality of understanding human behavior and its role in creating possible fraud threat vulnerabilities and addresses it in the fraud architecture framework.

Percentage of Duties	Essential Functions
35%	Applies state-of-the-art cybersecurity, fraud, privacy and vulnerability management best practices to design and develop enterprise-wide protection architecture that can identify, address and mitigate fraud and vulnerability risks. Includes the consideration of the following key information cybersecurity practices in the conceptualizing, planning and design of the EDD's cybersecurity, fraud and vulnerability architecture: • Alignment of Information Security Program and activities with Fraud Prevention measures in the organization • Conducting a Fraud Risk Assessment in the context of Information Security Threats – from Internal and External perspective • Identification, design and implementation of critical People, Process, and Technology Controls required to protect the organization, staff and its customers from fraud. • Implementing proactive monitoring and detective mechanisms to predict frauds through early warnings. • Formulating "use cases" by collecting intelligence through internal and external sources of information to detect potential fraud for a timely response. • Protecting information from internal and external threats through Confidentiality, Integrity, and Availability Controls, ensuring only authorized parties have access and authority to view and change the information and its status, with adequate audit trail. • Developing and performing incident response plans for handling potentially fraudulent activities due to information security breaches, where fraud management, investigation, legal and HR teams are involved. • Developing and implementing specific Technical and Procedural Controls for all online channels to be resilient to fraudulent activities. • Promoting Privacy awareness and ensuring compliance with privacy rules, in all design solutions and data sharing
30%	Provides mastery-level expertise in conceptualizing and designing enterprise-wide protection architecture to achieve compliance with applicable federal, state, local and industry legal, statutory, and regulatory requirements. For example, SAM 5300, SIMM 5300xx, FedRamp and IRS Pub 1075 vulnerability assessment requirements for EDD IT System interaction with Federal Taxpayer Information (FTI).
30%	Creates or facilitates standards in partnership with other ITB teams for all IT assets, such as routers, firewalls, LANs, WANs, VPNs, CLOUD and other network devices. Designs policies, procedures and processes for ongoing assessments to ensure that all firewalls, VPNs, routers, servers, CLOUD security processes, compliance frameworks are reviewed and approved before installation and perform as expected. Tests and ensures that the final security mechanisms supporting implementation work as expected. Reviews Information Security fraud and vulnerability incidents to identify any connection with ineffective Information Security controls, or weakness in people, process or technology controls associated with valuable business data. Synthesizes findings to develop robust and resilient fraud and vulnerability countermeasures to include in the architectural design.

Civil Service Classification
Information Technology Specialist III

Position Number
280-390-1405-001

Percentage of Duties	**Marginal Functions**
5%	Performs other responsibilities as needed

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: *Click here to enter text.*

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

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

5. SUPERVISION EXERCISED:

(List total per each classification of staff)

N/A

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

	PMG Analyst Initials	Date Approved
☒ Duties meet class specification and allocation guidelines. ☐ Exceptional allocation, STD-625 on file.	dmg	7/26/2023

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