Employment Development Department
State of California

☒ Current
☐ Proposed

POSITION STATEMENT

1. POSITION INFORMATION

CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Specialist II	Senior Cybersecurity & Fraud Engineer
NAME OF INCUMBENT:	POSITION NUMBER:
VACANT	280-390-1414-xxx
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Cybersecurity Operation & Fraud Center	
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division	Information Technology Manager I
BRANCH:	REVISION DATE:
Information Technology Branch	3/15/2024

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.)

Occasional overnight travel may be required.

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 I over the Cybersecurity Operation and Fraud Center, the IT Specialist II engineers, designs, develops, implements, and maintains information security related systems, policies, procedures, and practices that support enterprise cybersecurity and fraud activities. The IT Specialist II ensures these policies, procedures, practices, and systems incorporate and comply with applicable federal, state, local, and industry legal, statutory, and regulatory requirements including all associated hardware/software components and confidential and sensitive data used at the Employment Development Department (EDD). The incumbent applies cybersecurity and fraud detection and

countermeasures to monitor for possible data and system threats and vulnerabilities; and monitors the proper application of privacy protection processes to identify, address, and mitigate suspected disclosure and fraud incidents, in addition to inappropriate access and breaches of Personally Identifiable Information (PII) and Federal Tax Information (FTI). The IT Specialist II will demonstrate a depth of leadership and expertise in the performance of their duties.	
Percentage of Duties	**Essential Functions**
35%	In a lead and advisory capacity, performs engineering level technical tasks in support of the Cybersecurity Operations and Fraud Center regarding cybersecurity and fraud related issues. Performs the following: • Engineers, designs, develops, implements, and maintains security related architecture solutions, systems, tools, policies, procedures, practices, and documentation to support statewide enterprise cybersecurity operation and fraud activities. • Performs Linux and Windows security systems engineering, architecture design, configuration, coding and scripting development, patching, hardening security framework controls, principles, standards, and procedures. • Performs cloud security systems engineering, architecture design, configuration, coding and scripting development, code review ensuring standards and compliance, patching, and security research analysis to enhance the efficiency and effectiveness of cybersecurity and fraud operations. • Produces, formalizes, and maintains technical documentation and artifacts, configures security rules, database/dataset queries and alerts, monitors, and manages cloud, network, and endpoint events and data, and operational guides for security controls for EDD’s enterprise security information and event management, system logging, and security incident response. • Designs and develops security and fraud related technical documentation for enterprise business processes, applications, technology, and information security infrastructure and networking. • Serves as a technical security and fraud engineer for digital forensic services on enterprise cybersecurity and fraud systems and tools. • Collaborates with business units and IT branch (ITB) divisions in performance of cybersecurity fraud and risk assessments to identify security risks, recommend IT solutions, and documenting changes as proactive measures to control to counteract risk of fraud and/or breaches. • Designs new technologies and secure solutions to support fraud detection security requirements to align with strategic planning for EDD’s information technology enterprise and its customers, business partners and vendors. • Collaborates with Information Technology application and infrastructure staff in system design, modification, upgrade, and implementation projects pertaining to fraud; and information breach detection, prevention, and mitigation; and the development and deployment of robust and sustainable cyber security countermeasures to assess and test EDD’s IT applications and systems for potential weaknesses that could be exploited. • Engages in design, development, and usage of tools to detect malicious activity at the user, admin, host, and system level. Develop and maintain the log repository and advise the IT Manager I on logistics and safeguarding of data. • Configures and reports application monitoring and statistics. • Conducts technical IT forensic fraud investigations into suspicious activities to confirm or rule out fraudulent behavior.

	• Participates in IT change control and change management relevant to the development of cybersecurity and fraud operational systems. • Monitors and conducts audits of system fraud and breach detection and identification capabilities. Verify stability, interoperability, portability, security, or scalability of system fraud and breach detection and prevention architecture, e.g., test for fraud and/or breaches of IRS Publication 1075 vulnerability assessment requirements for EDD IT System interaction with Federal Tax Information (FTI). • Makes timely reports to the Cybersecurity Operations and Fraud Center IT Manager I regarding cybersecurity and fraud related issues, and remedial mitigation actions taken. Performs as a lead project security expert and advisor to project management, project teams, and system owners for technical project documentation utilizing state recognized requirements, best practices and techniques in the planning and deployment of project cybersecurity infrastructure, enhancements, suspicious activity monitoring tools, along with facilitating staff training and development opportunities to proactively address potential cybersecurity fraud, breach detection, vulnerabilities, testing, policy documents/requirements and documentation of findings, and modernization.
25%	**Cybersecurity Incident Response** Responds to the more complex escalated enterprise threats, vulnerabilities, and incidents by investigating scope, impact, and troubleshooting to resolve issues and close with root cause analysis. Acts as a technical engineering lead and mentor for less experienced staff for department security system assessments. Engineers and supports the evaluation and testing of cybersecurity and fraud related hardware and software. Contain and mitigate cybersecurity incidents to minimize damage and prevent further compromise. Performs the more complex engineer level technical review and analysis of EDD cybersecurity and fraud systems to ensure applicable enterprise security policies and standards are adhered to. Routinely reviews information systems to ensure they are compliant with National Institute of Standards and Technology (NIST) SP 800-53, Statewide Security Policies, Statewide Information Management Manual (SIMM), the State Administrative Manual (SAM), IRS Publication 1075, EDD ITB Technical Circulars, and current industry best practices for addressing each control. Defines any issues found and coordinates with team members and other stakeholders, including governance policy groups, to resolve the more complex internal EDD and external audit findings. Documents completed work, including how the finding were resolved and the date the finding were resolved to meet expectations and requirements of both internal and external auditors.
20%	**IT Cybersecurity and Fraud Threat Hunting** Facilitates threat intel to assist with identification of countermeasure recommendations to offset potential and expected threats to guard against benefit fraud risks to meet the increasing need in cyber risk management and strengthen the EDD cybersecurity posture. • Proactively identifies more complex threats and vulnerabilities, monitors security alerts, conducts investigations, leads and mitigates active security incidents. • Proactively search for signs of hidden cybersecurity threats and advanced persistent threats that could evade automated detection. • Serves as a cybersecurity threat and vulnerability hunting and incident response expert for system information and event management, extended endpoint detection and response, and security orchestration automation and response. • Incorporates threat intelligence feeds and indicators of compromise to enhance cybersecurity threat detection capabilities.

	• Analyzes security events and incidents to understand and document attack patterns and tactics used by threat actors. • Correlates data from various sources to identify the more complex, multi-stage attacks. • Conducts forensic analysis and evidence gathering for systems. • Maintains an awareness and inventory/listing of all EDD systems that process, store, transmit, or display PII and FTI. • Develops procedures and workflows for incident handling, particularly for analyzing fraud and/or information breach incident-related data and determining the appropriate response. Monitors for persistently evolving cyber-attacks and benefit fraud tactics being utilized by individuals, organized criminals, and foreign nation state; identify solutions for fraud mitigation and to improve cybersecurity and suspicious event monitoring, response, resiliency, collaborating with HR, legal, law enforcement, state and federal authorities. • Collaborates with business units and ITB divisions in monitoring and maintenance of Business Continuity and Disaster Recovery policies and procedures for resumption of all operations in the event of cybersecurity breaches. Partner with IT Project Management for inclusion of cybersecurity and fraud prevention capabilities in the development or updating of project plans for IT projects. • Partner with Project Managers and system owners in leading and assisting project teams on State, and EDD frameworks which may include departmental project management methodologies to ensure project compliance with State fraud policies.
10%	Advise management of cybersecurity (e.g., SIEM, Machine Learning, Artificial Intelligence, etc.) of solutions needed to effectively carry out cybersecurity operations and fraud center functions. Ensure hardware is compatible with EDD cybersecurity systems, capabilities, and needs. Provide expertise and leadership when management is unavailable. Participate in technical meetings and strategy planning throughout EDD as needed.
Percentage of Duties	**Marginal Functions**
5%	Invests in personal development through continuous education to maintain position related knowledge in the IT field with the emphasis in cybersecurity and fraud services. The incumbent will also focus on promoting and advocating the foundational information cybersecurity and fraud system principles of confidentiality, integrity, and availability throughout EDD.
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: 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)

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

Classification and Pay (CPG) Approval

☒ Duties meet class specification and allocation guidelines. ☐ Exceptional allocation, STD-625 on file.	CPG Analyst Initials	Date Approved
	dmg	5/21/2024

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