Employment Development Department
State of California

☒ Current
☐ Proposed

POSITION STATEMENT

1. POSITION INFORMATION	
CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Specialist II	Senior Vulnerability Management Specialist
NAME OF INCUMBENT:	POSITION NUMBER:
Click here to enter text.	280-390-1414-021
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Cybersecurity Operations / Cyber Defense & Response	
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cybersecurity Division	Information Technology Manager I
BRANCH:	REVISION DATE:
Information Technology Branch	8/22/2023

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.)

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 general direction of the Information Technology Manager I, the Information Technology Specialist II acts as the primary departmental resource responsible for providing expert technical and analytical expertise while planning, developing, and implementing access and collection gaps that can be secured through cyber collection and/or preparation activities.

The Information Technology Specialist II is responsible for overseeing and managing the identification, assessment, and mitigation of security vulnerabilities within an organization's systems, applications, and networks. This role involves leading a team to perform vulnerability assessments, analyzing the results, prioritizing risks, and collaborating with other IT and security teams to ensure timely resolution of

vulnerabilities. Additionally, the specialist may develop and refine vulnerability management processes, stay updated on emerging threats, and provide guidance for remediation strategies. Communication skills are crucial to effectively convey risk assessments and mitigation recommendations to relevant stakeholders.

The incumbent contributes toward the growth of the Information Technology Branch into a customer-focused service organization by following Branch Cultural principles and by providing constructive feedback to others within the Branch regarding the application of those principles.

Percentage of Duties	Essential Functions
30%	Responsible for implementing and optimizing the organization's vulnerability management program. This involves defining vulnerability scanning scope and schedules, configuring and tuning scanning tools, interpreting results, and driving the remediation process. Set policies and metrics to mature the program. Minimize the organization's exposure to cyber threats by proactively finding and mitigating vulnerabilities. Monitor threat intelligence feeds to stay on top of vulnerabilities being targeted in the wild. Advise IT leadership on inherent risk associated with open vulnerabilities and prioritize remediation accordingly.
25%	Researches and maintains an expert knowledge of information security principles, industry best practices and applicable compliance regulations. Maintain a strong understanding of the security controls defined in National Institute of Standards and Technology (NIST) SP 800-53, State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), IRS Publication 1075, and current industry best practices for addressing each control, including the technical levels, administrative/policy, and physical security of each. That knowledge also includes understanding of the design and selection of technical solutions. Independently researches and understands highly complex technical issues which impact security of departmental data, study existing and emerging Federal and State requirements, and studies and understands the complex business processes and applications within the Employment Development Department (EDD).
20%	Plan and conduct a variety of manual assessments to identify vulnerabilities, including penetration testing, web application security assessments, social engineering, red team exercises, and code review. Scope each assessment, determine appropriate tools and techniques, analyze findings, and report detailed remediation steps. Validate scan results and find additional vulnerabilities not detectable through automated scans. Partner with IT and development teams to drive remediation based on severity, exploitability, and impact to the organization. Track remediation tasks, verify fixes, and report on status.
15%	Lead and mentor Vulnerability Management Specialists (IT Specialist 1). Responsibilities include monitoring, gathering, and analyzing lessons learned by VMG Technical staff, documenting the lessons into a central repository for future reference, and overseeing staff use of the designated ticketing system to convey requests for remediation planning and track cybersecurity advisories. Assists and participates in security awareness and education campaigns to foster enterprise wide understanding of efforts regarding higher levels of security maturity related to individual EDD projects, programs and staff activities.
Percentage of Duties	**Marginal Functions**
5%	Invests in personal development through continuous education to maintain position related knowledge in the information technology field with the emphasis in infrastructure services. The incumbent will also focus on promoting and advocating the foundational information system principles of confidentiality, integrity, and availability.

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: Occasionally - activity occurs < 33%	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 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)

Lead and mentor lower-level IT Technical (IT Specialist I) staff in the Vulnerability Management Group

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: *Click here to enter text.*

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.	FNB	8/21/2026

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