STATE OF CALIFORNIA
Franchise Tax Board

Proposed

HR Date: 12/15/2022

HR Initials: jcs

Duty Statement

Request for Personnel Action (RPA) Number 2223-01900	Effective Date
Classification Title Information Technology Manager I	Position Number 564-184-1405-001
Working Title Security Operations Center (SOC) Manager	Bureau and Section Privacy, Security and Disclosure Bureau (PSDB)

Our mission is to help taxpayers file timely and accurate tax returns, and pay the correct amount to fund services important to Californians. In order to support this mission, FTB employees strive to develop in CalHR's Core Competencies: Collaboration, Communication, Customer Engagement, Digital Fluency, Fostering Diversity, Innovative Mindset, Interpersonal Skills, and Resilience. Core competencies are the knowledge, skills, and behaviors which are foundational to all state employees regardless of classification.

General Statement

Under the general direction of the Security Operations Section Manager, the incumbent acts as the technical security expert and manager for Intrusion Detection and Compliance monitoring at Franchise Tax Board (FTB). The incumbent will have technical responsibility for planning, organizing, coordinating, directing and controlling the direction of the 24 x 7 Security Operations Center (SOC) at FTB. The incumbent will lead the efforts in the researching and identification of information security trends and technologies. All work is performed within the framework of the department's mission and values and is geared toward improving the effectiveness and efficiency of the department's business programs. The Functions of this position encompass the Information Technology (IT) Domain of Information Security Engineering.

Essential Functions

Percentage	Description
50%	**Management of SOC Functions and workloads** • Manage 24x7 team and provide leadership to technical staff in the unit on highly technical and sensitive work related to SOC functions; Nework Monitoring/Threat Hunting, Vulnerability Management, Admistration of SOC tools and Incident Response. • Serves as the primary expert and resource in providing support and mentoring while managing the work of senior level staff, setting priorities, scheduling work assignments, and making adjustments as necessary due to changing priorities. • Monitors assignments to ensure timely completion and mentors team efforts to ensure they complete their efforts on schedule and in conformance with security policies and procedures. • Work with staff on complex technical issues including troubleshooting of system issues and ensure that senior management are aware of issues that impact FTB business processes. • Manage the recruitment, hiring, training and administrative processes in support of 24 x 7 team. Manage staff resources to ensure staffing levels in support of the Bureau's customers and mission. • Assesses fiscal needs and identifies budgetary needs to assure effective use of resources and sufficient funding for project success. • Works with SOC supervisors and technical staff to respond to identified threats and security violations to departmental systems that may result in unauthorized intrusions, misuse of system resources, or other anomalous network activity • Analyzes activity to determine if events are actual attacks or false positives, and the type of response or corrective actions necessary. • Tracks and verifies resolution of identified events, and notifies appropriate departmental resources to ensure timely notifications to control agencies where required. • Plans, prepares, performs and evaluates vulnerability scans of FTB systems and work with

Percentage	Description
	technical staff in resolving deficiencies. - Set stategic goals for SOC and ensures they are aligned with Section and Bureau goals.
30%	**Implementation of FTBs future IT Security Strategy including Policy and Standard Development** - Be the leader in the most complex Information Security projects. Directs subordinate staff in the plan, design, test, implementation and maintenance of project deliverables. Perform research on the most complex Intrusion Detection and Compliance monitoring security issues. - Responsible for developing complex computer system models to improve the detection of illegal system accesses and activities. - Play a major role in the development of IT security polices and standards including implementation approaches and plans. - Leads department wide teams analyzing and determining solutions for implementing of security best practices and mitigation of compliance issues and potential security breaches, including plan development. Present findings and proposed solutions to senior and executive management
15%	**Technical Consultation to FTB Senior Technical Staff and Senior Management** - Identifies and assembles necessary resources to support the Information Security portion of complex computer technology projects. - Maintains an extensive knowledge and up-to-date perspective on evolving Intrusion Detection System / Intrusion Prevention System / Vulnerability management and Security trends, standards, and best practices. - Stays abreast of cyber-terrorism threats to the Department's information resources and from activities related to unauthorized intrusion attempts and misuse of system resources. - Participate as a Cybersecurity Incident Response Team (CIRT) back up captain to mitigate threats to network systems and recommend actions to secure system resources.

Marginal Functions

Percentage	Description
5%	- Work closely with Privacy, Security and Disclosure Bureau management team build strategy and vision of FTB's Information Security Program. Collaborate on building and defining Security Operations Sections strategic goals.

Employee: I confirm that I have read and understand the described duties and functions of this position.

Name (Print) Signature Date

Supervisor: I certify that the above information accurately represents the described duties and functions of this position.

Name (Print) Signature Date