Duty Statement

☐ Current ☒ Proposed

RPA Number:	Classification Title: IT Specialist II	Position Number: 673-860-1414-031
Incumbent Name:	Working Title: Information Security Analyst	Effective Date: Click or tap to enter a date.
Tenure: Permanent	Time Base: Full-Time	Intermittent Hours Per Month:
Division/Office: Office of Information Services	Section/Unit: Security Operation Center	Reporting Location: HQ / I Street
Supervisor's Name: Gareth Bevan	Supervisor's Classification: IT Manager II	CBID: R01
Confidential Designation: ☐ Yes ☒ No	Designated Position for Conflict of Interest: ☒ Yes ☐ No	Position Telework Eligible: ☒ Yes ☐ No
Supervision Exercised: ☐ None ☒ Lead		

General Statement

The Security Operation Center (SOC) has the responsibility for managing and reporting security incidents; developing and maintaining information security and privacy plans, policies, processes, procedures, and standards; risk management; security training and awareness; vulnerability detection and management; information security operations; and providing information security consulting services for implementing new information technology products, projects, and systems. The section is also responsible for Identity and access management and its integration into California Air Resources Board's (CARB's) applications.

Competencies

All employees are responsible for understanding and demonstrating the core competencies of collaboration, communication, customer engagement, digital fluency, diversity and inclusion, innovative mindset, interpersonal skills, and resilience.

Position Description

Under the general direction of the Information Technology (IT) Manager II, the incumbent provides technical expertise to architect, design, develop, and supports the complex CARB business applications and Customer Relationship Management (CRM) systems. The incumbent serves as a well-versed CRM developer for CARB business processes, ensuring platform integration meets business needs and technical requirements including custom solutions when needed to meet needs. In collaboration with project managers, business owners, subject matter experts, and co-developers

(state and contracted), the IT Specialist II leads a variety of IT activities that span the full software development lifecycle and systems integration activities. The IT Specialist II's professionalism, team leadership, and software expertise lead to superior customer satisfaction and delivery of products and services that meet or exceed the customer's expectations.

The incumbent will act as a System Architect, lead developer, and systems integration specialist. The incumbent works both independently and cooperatively with other IT and program staff performing complex work around analysis, design, planning, and implementation along with providing high-level guidance and direction using a holistic approach for the successful development and execution of strategy. The IT Specialist II works primarily in the Information Security domain.

INFORMATION TECHNOLOGY DOMAINS:

☐Business Technology Management
☒ Information Security Engineering
☐ IT Project Management
☐ Software Engineering
☐ Client Services
☐ System Engineering

% of Time	Essential Functions
40%	Act as a Vulnerability Management Specialist. Plan, design, and maintain CARB's enterprise vulnerability management processes across Windows, Linux, cloud, and laboratory systems. Identify, analyze, and remediate security vulnerabilities using tools such as Rapid 7, Azure Arc, Microsoft Defender, System Center Configuration Manager, Intune, Armis and Tanium to ensure systems remain secure and compliant. Define standards for vulnerability management. Perform continuous scanning and analysis, including Defense Information Systems Agency (DISA), Security Technical Implementation Guide (STIG) assessments and Security Content Automation Protocol (SCAP) scanning, to verify system configuration baselines and detect deviations. Conduct port scanning, review network protocol behavior, and assess exposure to unauthorized access or insecure services. Use knowledge of application development stacks, including software dependencies and third-party libraries, to understand how vulnerabilities arise in modern applications and how they impact CARB systems. Support staff and system owners by evaluating vendor-bundled components, determining remediation options, and recommending compensating controls where direct patching is not possible. Use tools such as Threat Locker to manage application control, enforce least privilege, and reduce the attack surface on endpoints. Develop and refine CARB's vulnerability-management approach for laboratory systems, taking into account specialized equipment, operational constraints, and vendor requirements. Partner with IT Operations, SOC, DevOps, and program teams to ensure vulnerability-management activities integrate smoothly into

	monitoring systems, patch cycles, project planning, incident response, and operational workflows. Gather data from vulnerability scanners, reports, dashboards, and asset inventories to produce clear and actionable metrics for leadership. Prepare summaries of remediation progress, backlog trends, compliance levels, and exceptions requiring approval. Generate reports that support risk-based decision-making and help maintain alignment with federal, state, and CARB security mandates. Use AI-assisted tools to improve the speed and quality of vulnerability triage, pattern recognition, asset correlation, and remediation recommendations. Apply these capabilities to large datasets across cloud and on-premise environments to enhance accuracy and efficiency. Collaborate with IT teams, security teams, and business units to ensure vulnerability-management priorities align with organizational goals and mission-critical needs. Provide guidance, documentation, and support to system owners and end-users to strengthen patch hygiene, improve system configurations, and reduce exposure to security threats. Continuously improve CARB's vulnerability-management environment by staying updated with current security developments, tool capabilities, and industry best practices. Collaborating with various stakeholders, including IT teams, security teams, and business units, to align the vulnerability management strategy with organizational goals.
25%	Oversee the review and analysis of software and hardware and provide recommendation approvals to the Information Technology Operations and Support Branch Manager, Chief Information Officer, and CARB's Information Security Officer based on CARB end users' requests to OIS, following existing software and hardware standards and providing alternate solutions. Ensures software/hardware is compatible with, and interfaces well with, CARB's existing proposed hardware infrastructure and software. Works closely with CARB's CIO, ISO, IT Specialist I and IIIs to ensure any new or existing software does not create security risks to CARB's technical environment. Manages, reviews, and ensures CARB end users utilize software licenses appropriately according to end user license agreements (EULAs). Works closely with management to rectify immediately any discrepancies found in breach of EULAs and ensures software license compliance sustains any type of internal/external audits. Collaborates with the Technical Support and Enterprise Systems Management Sections that publishes software updates; tracks and projects completion dates of all software to be updated and documents progress status reports for OIS management monthly, ensuring CARB is secure from any potential malware viruses due to patching, mitigating controls, or configuration updates.
10%	Works closely with CIO, ISO, IT Supervisor II and SDSB Manager to run vulnerability/security scans within CARB's environment and analyzes, translates and reports scan findings to OIS management. Develops a remediation plan and follows the remediation progress; presents vulnerability reports to OIS management. Monitors, reports, and educates OIS staff on security findings and remediation options as required. Assists with remediation of security findings

	where necessary. Research and present new security threats and mitigation strategies to OIS management. Attend meetings for applications and new/proposed infrastructure to drive security awareness as well as to make security recommendations. Maintains vulnerability scanning hardware and software and manages scanning product support and upgrades when necessary. Maintains data classification software and upgrades when necessary. Develop automation scripts as needed to maintain an efficient environment. Troubleshoots network issues in partnership with the networking team.
10%	Develop, document, diagram, and maintain standard operating best practices and procedures to manage and protect information assets held privileged at CARB. Reviews security and application audit logs for malicious activity, network anomalies, and inconsistencies. Help correlate logs in Splunk and investigate security notifications from outside agencies. Review requests for web proxy exceptions and manage CARB employee access to specific web domains. Research, recommend, and apply appropriate web proxy policy for CARB employees based on job function and business justification. Reviews and maintains exceptions to CARB's web proxy policies.
10%	Research, analyze, recommend, and implement additional software or hardware components to be procured, developed, tested, implemented, and deployed to CARB end users enterprise wide. Research, monitor, maintain, and support a variety of modified and customized off-the-shelf software database products, including, but not limited to, Defender Endpoint Protection, WebSense, Qualys, O365, and Thycotic secret server.

% of Time	Marginal Functions
5%	Assist Security Operations Center with IT Security Awareness training and security awareness campaigns. Help research, create, and distribute IT security awareness topics monthly to educate CARB employees on emerging security threats. May perform other duties within the scope of the classification as required.

Typical Physical Conditions/Demands

Work is performed in a climate-controlled office environment.
Requires prolonged periods of sitting at a desk and working on a computer.
Involves frequent use of standard office equipment such as computers, phones, copiers, and printers.
May require occasional lifting and carrying of materials weighing up to 25 pounds.
Requires visual acuity to read and prepare documents and use a computer screen.

Typical Working Conditions

Work is performed in a climate-controlled office environment.
Involves prolonged periods of sitting at a desk and working on a computer.
May require frequent interaction with staff, stakeholders, or the public via phone, email, or video conferencing.
Noise levels are typically low to moderate.

May involve occasional travel to attend meetings or trainings.

Special Requirements of Position (Check all that apply):

☐ Duties may require pre-employment and routine screenings (background/criminal/fingerprint clearance, drug testing, fingerprinting, physical, etc.).

☐ Duties require participation in the DMV Pull Notice Program.

☐ Performs other duties requiring high physical demand. (Explain below)

☐ Requires repetitive movement of heavy objects and/or operation of heavy machinery or motorized vehicles.

☐ Travel up to _____ percentage

☐ Bilingual Fluency needed in _____(language)

☐ Other-

Supervisor Statement

I certify that this duty statement accurately describes the essential functions of this position. I have discussed the duties of this position with the employee and provided the employee with a copy of this duty statement.

Supervisor Name: Gareth Bevan	Supervisor Signature:	Date: Date

Employee Statement

I have discussed these duties with my supervisor and have been provided a copy of this duty statement. I certify that I have read, understand, and can perform the duties of this position either with or without reasonable accommodation*.

** Reasonable accommodation is any modification or adjustment made to a job, work environment, or employment practice or process that enables an individual with a disability or medical condition to perform the essential functions of his or her job or to enjoy an equal employment opportunity. (If you believe reasonable accommodation is necessary, check yes. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the Reasonable Accommodation Coordinator.)*

Do you need reasonable accommodation to perform the essential functions of this position? ☐ Yes ☐ No		
Employee Name:	Employee Signature:	Date: Date