STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF TECHNOLOGY

DUTY STATEMENT
TECH 052 (REV. 02/2018)

RPA NUMBER (HR USE ONLY)
26-017 PROPOSED

ALERT: This form is mandatory for all Requests for Personnel Action (RPA).
INSTRUCTIONS: Before completing this form, read the instructions located on last page.

Section A: Position Profile

A. DATE	B. APPOINTMENT EFFECTIVE DATE	C. INCUMBENT NAME
08/11/2026		Vacant

D. CIVIL SERVICE CLASSIFICATION	E. POSITION WORKING TITLE
Information Technology Associate	Product Analyst
F. CURRENT POSITION NUMBER	G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR)
695-331-1402-002	695-331-1401-xxx
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION	I. SUPERVISOR NAME AND CLASSIFICATION
Security Operations / Security Operations Center / Security Solutions Admin / Rancho Cordova PG1	Information Technology Supervisor II
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE)	K. POSITION REQUIRES:
MONDAY-FRIDAY 8:00 AM-5:00 PM/ DAY	**FINGERPRINT BACKGROUND CHECK** ☒ **YES** ☐ **NO**
	DRIVING AN AUTOMOBILE ☐ YES ☒ NO

Section B: Position Functions and Duties

Identify the major functions and associated duties, and the percentage of time spent annually on each (list higher percentages first).

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

Organizational Setting and Major Functions

Under general supervision of the Information Technology Supervisor II (IT Sup II), the Information Technology Associate (IT Assoc) will work with guidance from team leads including IT Specialist I and II's, working to assist various California Department of Technology (CDT) security and risk management functions. The IT Assoc will work in a team setting for ongoing maintenance and support of production security systems and services managed by Security Solutions.

Essential Functions

% of time performing duties

35%

Customer Engagement & Service Presentations

- Act as the initial point of contact for public sector organizations interested in cybersecurity services.
- Present the features, benefits, and operational model of continuous monitoring and threat detection services in a clear and accessible manner.
- Clarify roles, responsibilities, and expectations associated with service participation.
- Capture customer needs and maintain records of engagement and follow-up actions.
- Conduct introductory and follow-up meetings with public sector clients to present available security services through virtual meetings, email, instant messaging, and phone calls.
- Provide clear, professional explanations of technical service components to non-technical audiences.

30%

Technical Implementation and Customer Support

- Gather customer requirements and feedback to support service tailoring and continuous improvement.
- Maintain detailed records of customer interactions, commitments, and timelines.
- Lead customer onboarding processes, including scheduling, data gathering, and coordination with technical teams and vendors.
- Support integration of agency systems with monitoring platforms, including log source identification and data flow setup.
- Track onboarding milestones and ensure all requirements are completed in a timely and organized manner.
- Provide regular status updates to stakeholders and escalate technical or procedural barriers when necessary.

10%

Documentation & Administrative Support

- Maintain accurate and up-to-date service documentation, including onboarding materials, customer profiles, and implementation guides.
- Coordinate updates to FAQs, service runbooks, and communication templates.
- Assist in compiling metrics and reporting on customer onboarding status and service adoption.

10%

Cross-Team Coordination & Internal Collaboration

- Act as a liaison between customer agencies, internal service delivery staff, and third-party providers to ensure cohesive service implementation.
- Participate in internal meetings to provide customer perspective and feedback.
- Support internal process improvements related to service rollout and engagement workflows.

5%

Security Operations and Support

- Collaborate with IT Specialists, customers, and vendors to assist in maintaining security related systems and services.
- Assist in the implementation and maintenance of cybersecurity tools and technologies.
- Support compliance efforts related to NIST, IRS 1075, HIPAA, CJIS, and other regulatory frameworks.
- Collaborate with IT Specialist I and II's in largescale efforts such as department-wide risk assessments, compliance audits, technology evaluations, and document reviews as directed.
- Complete written analysis and reports as required.

5%

Professional Development

- Stay current with developments in cybersecurity services, IT project coordination, and customer engagement strategies.
- Attend relevant training sessions, conferences, and knowledge-sharing events as needed.
- Participate in developing and maintaining a working knowledge of cybersecurity technologies & techniques, operating systems, network protection technologies, cloud services, system architecture,systems development lifecycle, and risk management.

Marginal Functions

5%

- Perform other duties as required.
- Attend meetings and communicate professionally and positively.

Work Environment Requirements

The incumbent works in an office environment and is required to:

- **Successfully complete (pass) a fingerprint background criminal record check completed by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).**
- Operate a personal computer (word processor, spreadsheet, e-mail communication,presentation, and diagramming applications).
- Work some weekends and outside of normal business hours on a periodic basis.
- Carry and use a cell phone or mobile device and respond in a timely manner.
- Some travel between Rancho Cordova and Sacramento.

May be eligible for telework and when permitted incumbent is:

- Required to support a work from home environment.
- Expected to maintain a secure workspace within their home and support necessary logistical requirements to support remote video conferencing and remote work.
- Maintain a secure work from home environment for all work materials to ensure they are not misused, lost, damaged, stolen or improperly disclosed.

Allocation Factors

Supervision Received:
The IT Assoc works under the general supervision of the IT Sup II. The IT Assoc is expected to complete assignments independently as a technical specialist. The IT Assoc will assist in developing and executing project plans for assignments (including scope of work, identification of internal and external staff stakeholders as well as resources requirements). The IT Assoc has a responsibility to review progress, report problems, and provide recommendations (i.e., changes in priority or schedules). The IT Assoc is required to perform all duties and functions with a degree of independence.

Actions and Consequences:
The IT Assoc provides a working analysis for the selection of products and services offered to CDT customers. As a representative of CDT to its customers, the Government Operations Agency, and the Office of Information Security, a degree of professionalism and knowledge of security trends within the CDT customer base and within the industry are required. The IT Associate must adhere to the CDT change control requirements and processes.

The IT Assoc possesses knowledge of industry compliance requirements and trends including: FISMA/NIST 800-53, FedRAMP, IRS, CJIS, PCI and HIPAA requirements are essential. The IT Associate will effectively ensure that Security Solutions' products and services align with customer security requirements. The inability to perform this function would result in the delivery of inappropriate security services to CDT customers.

Personal Contacts:
The IT Assoc is in personal contact with a wide variety of technical, administrative and CDT management daily. External contacts include CDT customers, the Government Operations Agency, the Office of Information Security, various state and local agencies, and security vendors.

Administrative and Supervisory Responsibilities:
None.

Supervision Exercised:
None.

Other Information

Desirable Qualifications:

- Experience in planning and controlling customer account related activities.
- Experience in effectively communicating with customers and managing multiple customer relationships.
- Exposure to SIEM platforms or log management tools.
- Experience in KQL (Keyword Query Language).
- Experience in Cloud environments.
- Experience in Python, XML, and JSON.
- Ability to understand other scripting and markup languages (PowerShell, HTML, CSS).
- Experience in Unix or GNU/Linux.
- Knowledge in regular expressions (regex).
- Experience in system administration.
- Experience in cybersecurity technologies and related best practices.
- Experience in Windows and Linux operating systems.
- Experience of multi-location Data Center operations and technologies.
- Experience working with software defined networks concepts, Cloud computing, and Infrastructure as a Service methodology.
- Experience of NIST 800-53 and California State Administrative Manual.
- Experience evaluating new cybersecurity technologies for and making effective recommendations for their use.

	• Knowledge of California state IT and cybersecurity policies (e.g., SIMM, SAM). • Ability to apply analytical and problem-solving skills to identify, troubleshoot, and resolve technical issues effectively. • Ability to communicate effectively verbally and in writing as appropriate for the needs of the audience. • Ability to communicate effectively with a wide variety of individuals and audiences at different levels and with different backgrounds both inside and outside of the organization. • Ability to communicate technical information clearly, persuasively, and professionally to diverse audiences, both verbally and in writing.

INCUMBENT STATEMENT: I have discussed the duties of this position with my supervisor and have received a copy of the duty statement.

INCUMBENT NAME (PRINT)	INCUMBENT SIGNATURE	DATE

SUPERVISOR STATEMENT: I have discussed the duties of this position with the incumbent.

SUPERVISOR NAME (PRINT)	SUPERVISOR SIGNATURE	DATE
IT Supervisor II		