STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF TECHNOLOGY
DUTY STATEMENT
TECH 052 (REV. 02/2018)

RPA NUMBER (HR USE ONLY)
26-023 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

D. CIVIL SERVICE CLASSIFICATION	E. POSITION WORKING TITLE
Information Technology Specialist III	Information Security Architect
F. CURRENT POSITION NUMBER	G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR)
695-331-1414-007	695-331-1415-xxx
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION	I. SUPERVISOR NAME AND CLASSIFICATION
Office of Information Security/Security Operations/Security Operations Center/GC	Information Technology Manager II
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE)	K. POSITION REQUIRES: FINGERPRINT BACKGROUND CHECK ☒ YES ☐ NO; DRIVING AN AUTOMOBILE ☐ YES ☒ NO
MONDAY-FRIDAY / 8:00-5:00 (DAY)	

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 the administrative direction of the Information Technology Manager II (IT Mgr II), the Information Technology Specialist III (IT Spec III) serves as the Office of Information Security's (OIS) Lead Data Architect for the Security Operations Center (SOC). The IT Spec III is responsible for the architecture, design, development, integration, and management of the large-scale security data platform that supports the agency's threat detection, incident response, and cyber defense mission. The IT Spec III leads data architecture and data modeling efforts to establish efficient, secure, and scalable methods for collecting, storing, correlating, and reporting high-volume security telemetry across a multi-tenant environment, and designs the data lake/lake house foundation that enables advanced analytics, machine learning, and AI-enabled and agentic automation for security operations. This is accomplished through the delivery of services across IT domains including Software Engineering, System Engineering, Information Security Engineering, and IT Project Management, and through the IT Spec III's leadership of the on-premises AI compute platform used to fine-tune, evaluate, and serve the machine learning and large language models supporting Tier 1 security operations.

The IT Spec III works independently or collaboratively, and acts in a lead capacity to plan and coordinate technology solutions addressing the agency's most complex security problems, including the expansion of SOC services to additional state, local, and critical-infrastructure partners, and the engineering of AI-assisted detection, triage, and threat-hunting capabilities. Additionally, the IT Spec III solicits and considers internal and external customer input when completing work assignments in the Security Solutions Operations Unit, and maintains ongoing contact with technical, administrative, and managerial staff across CDT and customer organizations. The technologies supporting these functions include Microsoft Azure (Microsoft Sentinel, Log Analytics, Azure Data Lake Storage); Databricks, Delta Lake, and Apache Spark; Kusto Query Language (KQL); Microsoft Defender XDR; MS SQL Server and T-SQL; Python (including PySpark); data pipeline/ELT tooling; REST and GraphQL web services and APIs; JSON and XML; Power BI, Power Apps, and Power Automate; containerization (Docker) and version control (GitHub); large language model (LLM) and agentic AI frameworks; and Red Hat Linux and Windows Server.

% of time performing duties	Essential Functions
40%	**AI/ML Systems Engineering & Tier 1 Automation:** The IT Spec III designs, builds, and operates the on-premises artificial intelligence compute platform (GPU server infrastructure) used to fine-tune, evaluate, and serve the machine learning and large language models that support Tier 1 (T1) security operations, including

automated alert triage, enrichment, and analyst-assist capabilities. The IT Spec III establishes and maintains the model training and inference pipeline, including data preparation, fine-tuning, evaluation and guardrail testing, versioning, and deployment on state-controlled infrastructure, to keep sensitive security telemetry in-state and off commercial AI services, consistent with applicable generative-AI risk and data-handling requirements. The IT Spec III designs and engineers the data foundation that enables advanced analytics, machine learning, and AI-enabled and agentic automation for security operations and leads the integration of these capabilities into the SOC's detection, triage, and threat-hunting workflows. The IT Spec III manages the underlying compute, containerized workloads, storage, networking, capacity planning, and lifecycle for the on-premises AI system.

40%

Security Data Architecture Leadership:

The IT Spec III directs and oversees the design and establishment of the security data architecture, with the Microsoft Sentinel data lake in the Microsoft Defender portal serving as the state's primary security data platform. The IT Spec III provides management direction and expert guidance to staff responsible for designing and supporting security data models spanning multiple platforms, data sources, and environments (on-premises and cloud). The IT Spec III establishes data, schema, and query standards and ensures their consistent application. The IT Spec III assesses security operations goals and sets direction for how high-volume security telemetry is collected, stored, consumed, integrated, and managed across data entities, systems, and applications.

The IT Spec III oversees the evaluation of complex ingestion and structural requirements across network detection/IDS, endpoint, identity, and SIEM telemetry in a multi-tenant environment, and directs the optimization of data structures in the Defender data lake for detection, hunting, reporting, analytics, and cost-efficient retention. The IT Spec III leads and prioritizes the team's development of the most complex data solutions, from conceptual modeling through storage optimization, and establishes standards for Extract-Transform-Load/Extract-Load-Transform (ETL/ELT) and streaming ingestion used to integrate data from multiple security systems at scale. The IT Spec III serves as the accountable manager for security data architecture standards, and reviews and approves system and detailed design specifications, including system diagrams, entity relationship diagrams (ERD), data models, database and lakehouse schemas, access requirements, and data flow diagrams.

15%

Data Security, Privacy, Governance & IT Project Coordination:

The IT Spec III designs, documents, develops, and implements data architecture security and privacy controls spanning multiple IT platforms, including access control, encryption, and data-handling standards appropriate to sensitive multi-tenant security data. The IT Spec III documents data architecture policies, system requirements, and maintenance methodologies and procedures, and documents guidelines, standards, and processes to ensure data quality and integrity. The IT Spec III advises management on data architecture, governance and policy and provides expert guidance and oversight to ensure data management and software-licensing compliance. The IT Spec III assesses and plans for future cloud-based data platforms and recommends guidelines for infrastructure and software-licensing procurement. The IT Spec III coordinates complex information technology projects, including the expansion of SOC services to additional state, local, and critical-infrastructure partners, by defining project scope, objectives, schedules, resource plans, cost estimates, risk identification, procurement plans, roles and responsibilities, and communication. The IT Spec III advises management on the planning, development, implementation, and coordination of security data and platform initiatives, and provides technical training, mentoring, and knowledge transfer to SOC staff on all aspects of data architecture, systems analysis, troubleshooting, coding, testing, implementation, maintenance, and operations of data management solutions. The IT Spec III works as a project lead on other special projects and performs other duties appropriate to the classification.

Marginal Functions

5% Support and assist the SecOps Branch Chief as required to represent the Office of Information Security both internally and externally.

Work Environment Requirements

The IT Spec III works in an office environment and is required to operate a personal computer (word processor, spreadsheet, e-mail communication, presentation, and diagramming applications); use technical software for monitoring a variety of security-related items; and copy machine, fax machine, telephone system. **Must pass a fingerprint background criminal record check completed by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).**

Allocation Factors

Supervision Received:

The IT Spec III works under the administrative direction of the IT Manager II. Assignments are given in general terms with the desired results and timeliness being specified. The IT Spec III performs various phases of the activity including the detail development and scheduling of tasks.

Actions and Consequences:

The IT Spec III assists management in developing and maintaining confidentiality, integrity and availability of CDT and customer assets to ensure compliance with the State Administrative Manual and Federal mandates. The IT Spec III must use appropriate discretion and maintain confidentiality when processing confidential, sensitive or personal information. Failure to successfully implement these responsibilities could result in severe consequences including the loss or compromise of critical data or State IT assets

Personal Contacts:

The IT Spec III will have frequent, ongoing contact with a wide range of technical, administrative, and managerial staff within CDT and customer organizations, as well as senior-level IT staff, vendors, external entities, and stakeholders. These contacts occur regularly to coordinate technical activities, address operational and project needs, and support organizational and statewide initiatives.

Administrative and Supervisory Responsibilities:

None.

Supervision Exercised:

The IT Spec III does not supervise but may provide technical and project management leadership. This level may provide leadership, coordination, and oversight to CDT and statewide stakeholder groups to achieve security goals and develop and implement uniform security policies, procedures, and practices. The IT Spec III may lead workgroups, projects, or initiatives and provide direction and guidance to staff and stakeholders without having direct supervisory authority.

Other Information

Desirable Qualifications

In addition to evaluating each candidate's relative ability, as demonstrated by quality and breadth of experience, the following factors will provide the basis for competitively evaluating each candidate:

- Experience designing or supporting large-scale security data platforms, including multi-tenant or enterprise environments
- Experience understanding of SIEM concepts, security telemetry, log management, and data correlation strategies
- Experience using query languages or search engines to analyze high-volume security data (such as proficiency in KQL, SQL, or equivalent technologies)
- Experience building or maintaining data pipelines, streaming ingestion frameworks, or

	ELT/ETL processes • Experience architecting data lake or lake house environments, including schema design and optimization • Experience applying machine learning or automation concepts within security operations workflows • Experience planning, implementing, or supporting on-premises or cloud-based AI/ML infrastructure • Experience integrating data from diverse security platforms such as endpoint protection, identity systems, network detection tools, or SIEM/SOAR technologies • Ability to translate complex technical data concepts to non-technical audiences • Experience leading technical teams or providing subject matter guidance in data architecture or security engineering • Analytical skills, including the ability to identify patterns, detect anomalies, and evaluate data quality issues • Experience developing or maintaining data governance frameworks, including access controls, auditing, and compliance documentation • Ability to manage competing priorities across multiple complex projects • Experience with scripting or programming languages commonly used for data processing (such as Python, R, or equivalent)

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