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

PROPOSED

RPA NUMBER (HR USE ONLY)
22-309

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
4/28/2023		Vacant

D. CIVIL SERVICE CLASSIFICATION	E. POSITION WORKING TITLE
Information Technology Specialist III	IT Specialist III
F. CURRENT POSITION NUMBER	G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR)
695-533-1415-004	
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION	I. SUPERVISOR NAME AND CLASSIFICATION
Office of the Directorate / Critical Services / Rancho Cordova PG1.3	Tracy Lee, 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, 8:00AM - 5:00 PM, 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

The California Department of Technology's (CDT's) Office of the Directorate, Critical Service (CS) Program helps state entities evaluate the critical services they deliver with information technology (IT) systems and identify opportunities for system improvement to prevent failure or substandard performance.

Under administrative direction of the Information Technology Manager II (IT Mgr II), the Information Technology Specialist III (IT Spec III) serves as the Infrastructure Architecture lead at the mastery level in the evaluation and recommendation of enterprise technology systems and standards. The IT Spec Ill will work collaboratively with the CDT's Information Technology (IT) leaders and personnel responsible for managing the CDT Risk Assessment and Stabilization Program projects. The IT Spec III will be responsible for having a deep and thorough understanding of IT services, software, hardware, and technology stacks that cross many vendors to support the stabilization of critical IT services within the state. Responsibilities of this position will perform triage diagnostics on critical IT services, recommend stability-based corrective actions, and deliver triage consulting services. Components of the technical stack to be assessed shall include application suites, database, middleware, operating system, hardware, and monitoring solutions. The IT Spec III will baseline performance metrics for services within the stack and recommend processes to optimize and scale services. The IT Spec III will also provide an evaluation of the systems reliance on skills and subject matter expertise, maintainability, production stability, architectural alignment, and cloud suitability based upon industry best practices to determine the short- and long-term strategy for the service.

Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.)

% of time performing duties

40%

Lead Infrastructure Technical Specialist

The IT Spec Ill - Infrastructure Technical Specialist will lead and perform technical assessments of the stability and robustness of existing State enterprise IT systems, as identified for evaluation by the CDT, state leadership, the Governor's Office or other executive entity. The IT Spec III is expected to possess mastery level knowledge and expertise and is responsible for the following duties.

- Lead and work with cross-functional state and vendor teams to assess, evaluate and remediate existing State IT systems and services.
- Develop and maintain an expert knowledge of operating systems, network architecture and protocols, security devices, data base management systems, system design, implementation, and testing, as well as interoperability and interdependency issues.

- Assess and evaluate all components in the technology architecture stack, including application suites, databases, middleware, operating systems, hardware and monitoring systems.
- Identify architectural deficiencies that place the availability of the services at risk.
- Collect qualitative and quantitative data and analyze the data to identify root causes of poor system performance or failure that is within the scope of the IT system review.
- Lead risk assessments to evaluate security controls using extensive technology expertise of all layers of IT solution stacks and their interoperability, to determine application security defects and vulnerabilities.
- Conduct in-depth assessment into service delivery issues including technical and technology-adjacent factors.
- Prepare reports of technical findings and recommendations to be included in the Risk Assessment reports. Incorporate technical assessment and findings into overall Risk Assessment Report for CDT clients.
- Lead remediation efforts by working in liaison with CDT clients and vendor partners to implement solutions that address IT security vulnerabilities and risks found during the assessment of the system and service.
- Measure system performance of databases, middleware, application code, storage, transport, cloud hosted services, APIs, backups services and high availability solutions that may be included as components of enterprise solutions being assessed.
- Provide guidance on integrating the State's network and cloud Infrastructure network.
- Provide corrective action assistance and triage consulting services.
- Develop and maintain expert level knowledge of IT security frameworks, standards and regulations.
- Develop and maintain an advanced level of threat knowledge, analytic techniques and methods.
- Participate in the procurement and engagement of outsourced security resources if/as needed.

Establish Standards and Technical Assessment Framework

30%

The IT Spec III will establish standards and develop and maintain a diagnostic technical evaluation and assessment framework for use within Risk Assessment sprints and strike teams. The Framework must be standardized yet flexible to be applied to any IT system within state government.

- Establish IT Security framework for assessment and remediation efforts.
- Establish and deploy monitoring tools to assess system performance pre assessment and during the cause of remediation.
- Participate in critical systems evaluations and reviews that are conducted affecting State-wide cybersecurity incident response.
- Participate and or lead incident response and recovery initiatives affecting State-Wide threat management processes.
- Write after action recommendations from incident response initiatives.
- Lead post incident retrospectives affecting State-wide cybersecurity incident response.
- Maintain a high level of knowledge on existing and emerging cloud technologies and cloud and hybrid cloud frameworks
- Attend conferences, seminars, and meetings to keep abreast of new technologies of any kind that would replace older or problematic IT solutions and systems. New technologies include cloud services and the full range of software services and tools that the State could adopt to solve IT performance problems.
- Research, analyze, recommend and select technical approaches to address challenging development and integration problems with on-premises, cloud or hybrid environments.
- Perform research activities to identify emerging technologies and trends that may affect the enterprise solutions under review or being recommended to resolve systemic issues.
- Maintain awareness of vendor/product industry developments, regulations and trends and identify potential impacts to the enterprise.

% of time performing duties 20%

Maintain High Level Technical Expertise

The IT Spec III maintains advanced technical knowledge in all domains within the IT solution infrastructure and operational stack and uses this expertise to lead and train others in the Risk Assessment methods and processes. Technology domain areas include but may not be limited to: Windows and Linux operating systems; database services, system design and architecture; middleware; network connectivity.

- Lead other IT specialists, experts and consultants assigned to participate in the Risk Assessment strike teams and longer-term tiger teams responsible for analyzing and making recommendations for system improvements.
- Consult on the application of reference architecture, strategic directions for statewide users, based on trends, issues and findings of Risk Assessments conducted by CDT. Serve as a SME with contextual knowledge of the business model.
- Find the best technology solution among all possible to solve the existing business problems regarding infrastructure and cloud technologies.
- Conduct and actively participate in meetings related to design with clients and partners.

5%

Training

- Foster an innovative culture, promoting an open and proactive approach to collaboration.
- Meet with customers' architects/developers to assist in assessing the skills needed to be successful in their long-term IT modernization efforts.
- Work with management to develop training materials, programs, test environments and technology road maps for State IT organizations and staff as a result of Risk Assessment activities.

5%

Marginal Functions **(Percentages shall be in increments of 5, and should be no more than 5%.)**

Perform other job-related duties as required.

Work Environment Requirements

- **Must pass a fingerprint background criminal record check completed by the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).**
- May be required to travel to various offices and locations throughout the State and surrounding areas to provide client services and attend meetings, conferences and training.
- May be required to travel via private or public transportation including overnight lodging.
- May be required to carry a mobile device and be available by phone and/or email.
- May be required to work outside of normal business hours: periodic off-shift and weekend work.
- Works in an office environment operating a laptop, keyboard, mouse, monitor(s) and printers under non-natural lighting for prolonged periods.
- Must maintain consistent, predictable attendance.
- Professional business attire may be required.

Allocation Factors **(Complete each of the following factors.)**

Supervision Received:

The IT Spec III receives administrative direction from the IT Mgr II.

Actions and Consequences:

The IT Spec III is expected to demonstrate strategic technical leadership; act independently in their duties and advise on major decisions that can have an impact on the governance and policies related to Infrastructure Services and Cloud architecture. Poor recommendations and facilitation can create significant problems in the development of a system and result in project delays and over-expenditures. This is especially important for systems that provide critical services to the public or satisfy a legislative mandate.

Personal Contacts:

The IT Spec III works closely with department's technical personnel and will have frequent contact with other State executive staff, managers, and staff, as well as vendors to advise, plan, and provide recommendations to minimize risk that could affect the stability of services. The IT Spec III has frequent contact with State executive staff, and sub-organizations to ensure that state procedures are followed, and that critical issues and policies are well understood and acted appropriately upon. Represent the State in a way that will enhance public respect for and confidence in the employee and State Government.

Administrative and Supervisory Responsibilities: **(Indicate "None" if this is a non-supervisory position.)**
None

Supervision Exercised:
The IT Spec III does not supervise but may lead. The IT Spec III provides technical and project management leadership but does not provide day-to-day operational management or supervision. The IT Spec III has defined responsibility and authority for decision making related to projects or in advisory function.

Other Information

Desirable Qualifications: **(List in order of importance.)**

- Experience conducting incident response and recovery initiatives affecting State-Wide threat management processes.
- Expert level knowledge of security framework to policies, standards and regulations.
- Ability to exercise judgment when policies are not well-defined.
- Knowledge of incident response and handling methodologies.
- Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies.
- Knowledge of penetration testing principles, tools, and techniques.
- Knowledge of policy-based and risk adaptive access controls.
- Knowledge of security risk management.
- Extensive project experience, architecting, documenting, migrating and deploying IT solutions.
- Excellent verbal and written communication, time management, presentation, and organizational skills.
- Hands-on, technical subject matter expert with the ability to propose, present and influence architectural design ideas to executives and technical management and work with customers' developers, architects, and technical management.
- Ability to identify key trends and emerging technologies that can enhance or impact the solution architecture to maximize the value of the State's Infrastructure, Cloud and Hybrid offerings.
- Extensive knowledge and practical application experience working in advanced software-defined networks concepts, Cloud computing, and Platform as a Service methodology.
- Strong creative ability with an exceptional track record of innovation and hybrid cloud strategy generation.
- Ability to communicate, influence and work with a wide audience to help drive the target system architecture across the State's infrastructure and cloud systems portfolio.
- Customer-focused with an ability to learn and adapt quickly to new technologies and environments while being able to see and present the "big picture."
- Experience designing security from both a cloud architecture and Infrastructure perspective.
- Experience with git or other source control tools.
- Experience with performance analysis, troubleshooting and remediation techniques.
- Experience with networking principles and technologies (DNS. Load Balancers, Reverse Proxies).
- Knowledge of High Availability and Disaster Recovery principles, patterns and usage.
- Ability to adapt the role of architect to a modern DevOps environment with both pre- and post-development engagements.
- Ability to participate with a cross department-functional team to establish a cloud operational governance framework.

	• Excellent knowledge of routing protocols and their application. • Experience in technology strategy development. • In-depth knowledge of the State's IT operations. • Experience in performance engineering. • Experience in database, middleware, OS, hardware, monitoring solutions.

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