STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF TECHNOLOGY

DUTY STATEMENT

TECH 052 (REV. 02/2018)

PROPOSED

RPA NUMBER **(HR USE ONLY)**

24-072

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 07/03/2024	B. APPOINTMENT EFFECTIVE DATE	C. INCUMBENT NAME Vacant
D. CIVIL SERVICE CLASSIFICATION Information Technology Specialist II		E. POSITION WORKING TITLE Information Technology Specialist II
F. CURRENT POSITION NUMBER 695-332-1414-002		G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR)
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION Office of Information Security/ California Cybersecurity Integration Center/ Mather, CA		I. SUPERVISOR NAME AND CLASSIFICATION Douglas Novak, Information Technology Manager II
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE) MONDAY – FRIDAY/ 8:00AM – 5:00PM/ DAY		K. POSITION REQUIRES: 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 the general direction of the Information Technology Manager II, the Information Technology Specialist II (IT Spec II) is the Subject Matter Expert for all aspects of the administration and management of the Cal-CSIC Operational Technology (O/T) Lab equipment. The IT Spec II will be responsible for the advanced design, installation, testing, monitoring, maintenance, troubleshooting, and repair of a variety of industrial electrical, instrumentation, and controls devices and systems associated with the production, storage, transmission, and monitoring of a power substation. The IT Spec II will also assist with the administration and management of CAL-CSIC Linux systems, Windows systems, and cloud applications in Amazon AWS and Microsoft Azure. The position requires exercising a high degree of initiative and independence, demonstrating tact and good judgment. This includes adapting to changing priorities and working effectively in a high-paced, demanding environment. This position will require a background check via the California Department of Justice Live Scan and DHS/FEMA security clearance to fulfill the responsibilities of the job.

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

% of time performing duties

40%

O/T Lab Equipment and IT Management and Support

- Manage and lead the installation, maintenance, and configuration of networking and system infrastructure of the substation O/T Lab network and existing IT infrastructure.
- Manage Cal-CSIC O/T Lab and IT infrastructure by applying patches, firmware updates, and system upgrades as needed.
- Manage and optimize Cal-CSIC O/T Lab network, network devices & WAN connection.
- Manage and optimize Cal-CSIC IT network, network devices & WAN connection.
- Lead and oversee the full lifecycle management of the substation O/T Lab network and IT network.
- Participate as the Subject Matter Expert on the engineering analysis and planning of the Cal-CSIC O/T Lab network infrastructure.
- Lead technical support and implementation of both O/T and IT equipment.
- Provide input as the Subject Matter Expert on the architectural security designs for the O/T Lab network and provides consulting for Cal-CSIC management and the Homeland Security Division (HSD) Critical Infrastructure Protection (CIP) unit.
- Ensure equipment meets established ERCOT, NERC, PUCT, and California standards and codes.
- Interpret electrical schematics, wiring diagrams, technical manuals, and test results.

40%

O/T and IT Systems Security

- Lead the evaluation of O/T systems and IT systems for cyber risks, security controls, and vulnerability remediation activities.
- Maintain understanding of both O/T and IT security and related protocols to develop and improve O/T and IT related use cases and rulesets.
- Identify O/T and IT risks, problem-solves, and implement highly complex solutions by coordinating work in the Cal-CSIC O/T Lab and/or IT network and Cal-CSIC staff.
- Monitor Threat Intelligence received from multiple sources and participates in Threat Hunting initiatives and activities in the O/T Lab and IT infrastructure.
- Implementation of both IT & O/T security and related protocols to develop and improve both IT and O/T related use cases and rulesets.
- Manage and lead the implementation and coordination of actions needed to respond to identified vulnerabilities and zero-day exploits on both IT and O/T equipment.
- Gather, analyze, and interpret endpoint data in order to efficiently and effectively make actionable decisions for both IT and O/T security.
- Support improvements to tune and shape the incident management playbooks for both IT and O/T equipment such as processes, procedures, runbooks and supporting tools.
- Assist with system security plan (SSP) creation/reviews.
- Serve as backup administrator for both the IT and OT infrastructure.
- Assist with network and system audits for both IT and OT infrastructure.

15%

O/T and IT Research, Development, and Reporting

- Research and track current trends in operational technology.
- Review network configuration and monitoring tools (e.g. tcpdump, Wireshark, etc.).
- Prepare reports and give presentations to colleagues and management regarding both O/T and IT security and best practices.
- Review the Operational Technology Purdue model for ICS security and apply security measures where applicable.

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

5%

Miscellaneous Duties

- Perform other related duties as required to fulfill the Cal OES and CAL-CSIC mission, goals and objectives.
- Respond to ticket requests for assistance.

Work Environment Requirements

This position physically reports to the California Office of Emergency Services (Cal OES) at 10390 Peter A McCuen Boulevard, Mather, CA 95655. Work is conducted in a professional office environment. Business dress, according to current office policy, is required. This position requires the ability to work excess hours, to effectively work under pressure to meet deadlines, use of a computer to communicate and prepare written materials, and the ability to travel to meetings, training, and conferences at various locations.

Additionally, When requested to fill an operational assignment and until demobilized, the following duties will be performed and your regular duties may temporarily cease.

Emergency Operations – Activation/Operational Assignment up to 100% at various times:

- May be required to work in the State Operations Center (SOC), Regional Emergency Operations Center (REOC), Joint Field Office (JFO), Area Field Office (AFO), Local Assistance Center (LAC), or other location to provide assistance in emergency response and recovery activities. All staff is required to complete operational related training and participate in one of three Readiness Teams that rotate activation availability on a monthly basis if not assigned to an Operational Branch (e.g., Fire/ Law/ Region/ PSC Operations (Technicians)/ PSC Engineering (Engineers).
- May be required to participate in emergency drills, training and exercises.
- Must be able to work effectively under stressful conditions; work effectively & cooperatively under the pressure of short leave time; work weekends, holidays, extended and rotating shifts (day/night). Statewide travel may also be required for extended periods of time and on short notice.

- While fulfilling an operational assignment it is important to understand that you are filling a specific "position" and that position reports to a specific Incident Command System (ICS) hierarchy. This is the chain of command that you report to while on this interim assignment.
- On Call/Standby/Duty Officer (if applicable).
- May act as the on-call, standby or as a Duty Officer. If assigned, you are required to be ready and able to respond immediately to any contact by Governor's Office of Emergency Services (Cal OES) Management (including contact from the State of California Warning Center) and report to work in a fit and able condition if necessary as requested.

After hours:

- May occasionally be contacted for after-hours emergency support.
- May be required to work weekends, holidays, extended and rotating shifts (day/night).

Travel:

- A valid California Driver's License (CDL) is required.
- Required to operate a State vehicle during the course of deployment as part of employment. May be required to travel to respond to IR incidents at various sites within California.
- Statewide travel may also be required for extended periods of time and on short notice.

Training:

- Required to successfully complete all training related to the functions of the job.

Security Clearance:

- **Must pass a fingerprint background check completed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI). In addition, employee shall obtain a SECRET Homeland level security and maintain the clearance to work in secured areas. This position requires the employee to be a US Citizen or US Naturalized Citizen.**

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

% of time performing duties

Supervision Received:
The IT Spec II receives supervision from the CSIC MSB Chief, IT Mgr II, and may receive guidance from IT Manager I within Cal-CSIC.

Actions and Consequences:
Failure to effectively perform the duties of this position will result in the local, state, and federal entities' inability to ensure consistency and compliance with state and federal law, regulation, policies, plans and procedures. This could result in statewide impacts, including, but not limited to, loss of state and federal disaster assistance funding for the Cal OES, other state agencies, local agencies, county and city organizations, individuals and businesses impacted by disasters, regulatory security compliance, and negative audit findings for the Cal OES.

Personal Contacts:
This position will interact with all levels of staff including agency secretaries, departmental directors, Agency Information Officers, Chief Information Officers, Information Security Officers, Privacy and Disaster Recovery Coordinators, and stakeholders from other branches and levels of government, education, critical infrastructure sectors, National Associations, and private industry.

Administrative and Supervisory Responsibilities: **(Indicate "None" if this is a non-supervisory position.)**
The IT Spec II is responsible for project goals and objectives.

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

Other Information

Must have knowledge of the state and related federal laws, rules, regulations, policies and procedures. Must exercise good writing skills; follow oral and written directions, be responsive to the needs of the public and employees of the Cal OES, CDT and other agencies; analyze situations and take effective action using initiative, resourcefulness, and good judgment.

Consistent with good customer service practices and the goals of the Cal OES Strategic Plan, the incumbent is expected to be courteous and provide timely responses to internal and external customers, follow through on commitments, and solicit and consider internal and external customer input when completing work assignments.

<u>Desirable Qualifications</u>: (List in order of importance.)

CompTIA Security +, GIAC Security Essentials or equivalent certifications are desired.

Knowledge of:

- Knowledge of computer networking concepts and protocols, and network security methodologies.
- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Knowledge of cybersecurity and privacy principles.
- Knowledge of cyber threats and vulnerabilities.
- Knowledge of specific operational impacts of cybersecurity lapses.
- Knowledge of computer algorithms.
- Knowledge of encryption algorithms.
- Knowledge of database systems.
- Knowledge of organization's enterprise information security architecture.
- Knowledge of organization's evaluation and validation requirements.
- Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).
- Knowledge of resiliency and redundancy.
- Knowledge of installation, integration, and optimization of system components.
- Knowledge of human-computer interaction principles.
- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Knowledge of information security systems engineering principles (NIST SP 800-160).
- Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
- Knowledge of local area and wide area networking principles and concepts including bandwidth management.
- Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).
- Knowledge of microprocessors.
- Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
- Knowledge of operating systems.
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
- Knowledge of parallel and distributed computing concepts.
- Knowledge of policy-based and risk adaptive access controls.
- Knowledge of Privacy Impact Assessments.
- Knowledge of process engineering concepts.
- Knowledge of secure configuration management techniques.
- Knowledge of software development models (e.g., Waterfall Model, Spiral Model).
- Knowledge of software engineering.
- Knowledge of structured analysis principles and methods.
- Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.
- Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.

- Knowledge of system life cycle management principles, including software security and usability.
- Knowledge of systems testing and evaluation methods.
- Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
- Knowledge of the systems engineering process.
- Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)
- Knowledge of interpreted and compiled computer languages.
- Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.
- Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).
- Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
- Knowledge of circuit analysis.
- Knowledge of cybersecurity-enabled software products.
- Knowledge of various types of computer architectures.
- Knowledge of Personally Identifiable Information (PII) data security standards.
- Knowledge of Payment Card Industry (PCI) data security standards.
- Knowledge of Personal Health Information (PHI) data security standards.
- Knowledge of security management.
- Knowledge of an organization's information classification program and procedures for information compromise.
- Knowledge of countermeasure design for identified security risks.
- Knowledge of cryptology.
- Knowledge of embedded systems.
- Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.
- Knowledge of access authentication methods.

Skills in:

- Skill in creating policies that reflect system security objectives.
- Skill in designing countermeasures to identify security risks.
- Skill in designing security controls based on cybersecurity principles and tenets.
- Skill in designing the integration of hardware and software solutions.
- Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort).
- Skill in developing and applying security system access controls.
- Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
- Skill in evaluating the adequacy of security designs.
- Skill in writing code in a currently supported programming language (e.g., Java, C++).
- Skill in conducting audits or reviews of technical systems.
- Skill in applying security controls.

- Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
- Skill in integrating and applying policies that meet system security objectives.
- Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications).
- Skill in the use of design modeling (e.g., unified modeling language).
- Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Ability to:

- Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

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