|  |  |
| --- | --- |
| State of CaliforniaCalifornia department of technologyDuty Statement PROPOSEDTech 052 (Rev. 02/2018) | **RPA NUMBER (HR Use Only)** |
|  21-021 |
| **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 |
| July 26, 2021 |   | VACANT |
| d. CIVIL SERVICE CLASSIFICATION | e. POSITION WORKING TITLE |
| Information Technology Specialist II (IT Spec II) | Cyber Defense Analyst |
| F. Current Position Number | G. proposed Position Number (Last three (3) digits assigned by HR) |
| 695-332-1414-001 |  |
| H. office / section / unit / physical Location of Position | I. supervisor Name and classification |
| Office of Information Security (OIS/California Cybersecurity Integration Center (Cal CSIC)/Cyber Operations Branch (COB)/ Mather, CA  | David Lane, Information Technology Manager II (IT Mgr II) |
| J. Work Days / Work Hours / work shift (day, swing, grave) | K. Position Requires:  | fingerprint background check | [x]  Yes [ ]  No |
| Monday – Friday / 8:00AM – 5:00PM  | Driving an Automobile | [x]  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[x]  Information Security Engineering | [ ]  IT Project Management[x]  Software Engineering | [ ]  Client Services [x]  System Engineering |
|  | Organizational Setting and Major Functions |
|  | Under the general direction of the Mission Support Branch (MSB) Chief, Information Technology Manager II (IT Mgr II) and the functional direction of the Cyber Operations Branch (COB) Chief, IT Mgr II, the Information Technology Specialist II (IT Spec II) serves as the California Department of Technology’s (CDT’s) Cyber Defense Analyst of the California Cybersecurity Integration Center (Cal CSIC) Incident Response (IR) team as part of the Homeland Security partnership. The Cal CSIC serves as the central organizing hub of the state government’s cybersecurity activities. The Cal CSIC's mission is to reduce the likelihood and severity of cyber incidents that could damage California’s economy, its critical infrastructure, or public and private sector computer networks in the state. Within the Cal CSIC, the MSB provides the following functions: Business Operations; Cyber Policy & Strategic Planning; Vendor Management; Partner Integration; Information Technology (IT) Engineering; and Metrics Collection & Reporting. The MSB develops, implements, enforces, and maintains processes, practices, and (as needed) policies related to the Cal CSIC. The MSB ensures that the Cal CSIC is compliant with all applicable legal, statutory, regulatory, and best practice requirements. Within the purview of the Incident Response team for security operations people/process/technology triad, the Cal CSIC has five main objectives: 1. Identify the threats and vulnerabilities/weaknesses present within the protected Information Technology (IT) infrastructure. 2. Protect, through security technology and processes, the assets and data present within the protected IT infrastructure. 3. Detect threats or malicious events present within the protected IT infrastructure. 4. Respond to security incidents within the protected IT infrastructure. 5. And assist as appropriate in the recovery from malicious events within the protected IT infrastructure. |
|  | Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.) |
| % of time performing duties**40%**% of time performing duties**30%**% of time performing duties**15%****15%** | The IT Spec II’s responsibilities include cyber defense monitoring, tracking, and processing of incidents. The IT Spec II provides consultation and recommendations related to security incidents. Responsibilities include but are not limited to: * Monitors and researches security traffic for incidents and providing analysis to team leads.
* Designs and implements system access controls to maintain system security in accordance with information security best practices and standard IT operating procedures.
* Reviews software architecture and make recommendations regarding security, technical, and operational feasibility.
* Uses defensive measures and information collected from a variety of sources to identify, analyze, and report security events that occur or might occur within the network to protect information, information systems, and networks from security threats.
* Responds to security crises or urgent situations within the pertinent domain to mitigate immediate and potential security threats. Uses mitigation, preparedness, response, and recovery approaches as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant security response activities.
* Conducts security assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.
* Creates, enhances, and maintains IT software solutions using various programming languages to meet department security requirements and expectations with regards to efficiency and effectiveness.
* Designs and implements data models using system specifications and security requirements to provide for efficient data storage and retrieval in accordance with best practices.
* Designs testing methods, validation procedures, and execution plans to evaluate software functionality and security.
* Plans, designs, and implements the enterprise data models using standardized modeling tools to align technology solutions with security strategies
* Debugs software using various programming tools and systematic debugging methods.
* Architects, designs, develops, and implements software that adheres to organizational enterprise architecture ensuring secure, reliable, and accessible salutations.
* Reviews software code to ensure compliance with defined security standards.

The IT Spec II provides input for the incident response teams relating to the security aspects of the initiation, design, development, testing, operation, security, and defense of IT environments in order to address sources of disruption, ranging from natural disasters to malicious acts. Responsibilities include but are not limited to: * Researches, documents, and develops reusable cyber security defense procedures/ playbooks in responding to security incidents.
* Actively responds to security incidents using playbook and security techniques accordingly.
* Provides input to cybersecurity recommendations based on significant threats and vulnerabilities. Provides advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
* Coordinates in the testing, implementation, deployment, reviews, and administration of infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized security activities.
* Provides status and input to recommendations for courses of action to establish and ensure security compliance.
* Coordinates in development of procedures for incident handling, particularly for analyzing security incident-related data and determining the appropriate response.
* Analyzes business impact and exposure, based on emerging security threats, vulnerabilities and risks to recommend IT solutions.
* Assesses, develops, implements, and maintains a security and privacy training and awareness program, ensuring consistency with the organizations security risk management strategy and priorities.
* Categorizes the information system and the information processed, stored, and transmitted by that system.
* Designs new technologies, architectures, and secure solutions that will support security requirements and align with strategic planning for the enterprise and its customers, business partners and vendors.
* Develops and ensures security solutions and technical artifacts are in place throughout all IT systems and platforms.
* Develops and maintains the IT Contingency Planning Program including preliminary planning, business impact analysis, alternate site selection, recovery strategies, security, training and exercising to work within the overall Business Continuity Plan
* Monitors and assesses security controls in the information system on an ongoing basis, documenting changes, conducting security impact analyses, and reporting system security statuses to the organization.
* Performs vulnerability and security risk assessments to identify security risks and recommend IT solutions.

The IT Spec II provides assistance and technical advice on all phases of the project management and system development life cycles to ensure efficient and effective delivery of a unique IT product, service, or system is implemented for incident responses. The IT Spec II will assist in describing the scope of work, objectives, tasks and resources needed to successfully plan the IT projects for the organization’s mission. As part of the IT portfolio, the candidate must collaborate with its business partners, prioritize IT projects, collaborate in selecting high value opportunities to enhance services, and effectively and efficiently operate the organization’s IT resources. * Develops and manages the work breakdown structure (WBS) of IT projects.
* Develops or updates project plans for IT projects including information such as project objectives, technologies, security, systems, information specifications, schedules, funding, and staffing.
* Leads and supervises project teams, which may include business analysts, system engineers, security analysts, system architects, subject matter experts, test coordinators, external entities, and users on the State and departmental project management methodologies to ensure project compliance with State policies.
* Integrates information systems and/or subsystems as designed.
* Manages project(s) to ensure adherence to budget, schedule, and scope.
* Performs security risk assessments to develop response strategies in order to control or reduce risk.
* Determines the resources (time, money, equipment, staffing, etc.) required to complete the project.
* Develops implementation plans that take into consideration analyses such as cost-benefit or return on investment.
* Directs the conduct of integrated change control processes.
* Makes changes to identification of infrastructure configuration, security, and change management standards or requirements.
* Manages or oversees one or more IT security projects applying industry standards, principles, guidelines, methods, techniques, security, using planning, monitoring, processes, and controlling principles tools to deliver an IT product, program solution, service, or system.
* Prepares documentation using standard California Project Management Frameworks or Methodologies.

The ITS II collaborates in ensuring the incident response team adheres to the architecture, design, configuration, security, operation, and maintenance of systems per the entity and State standards.  The IT Spec II works with the incident response team in the discovery plan, design, configuration, administration, and sustainment of operations of a defined system. System elements can include work and recommendations in network, server, storage, operating system, database, program, hardware, and software. Responsibilities include but are not limited to: * Audits systems performance and serves as the escalation point for troubleshooting system components.
* Contributes to the planning of the overall organizational IT security strategy.
* Communicates with stakeholders to determine organizational needs.
* Creates and implements backup and recovery strategies.
* Conducts disaster and recovery analysis, planning, implementation, and administration for systems.
* Provides system components capacity planning to ensure system sustainability and security.
* Coordinates infrastructure system designs, modifications, upgrades, and implementation projects.
* Develops and implements standards and controls that ensure the security, reliability, and availability of system components.
* Monitors and conducts audits of system capacity, security, performances, and traffic analysis.
* Performs configuration management and releases management for system components.
* Verifies the stability, interoperability, portability, security, or scalability of system architecture.
* Designs, implements, and maintains system architecture across multiple platforms to best align technology solutions with security strategies.
 |
|  |  |
|  | 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:1. EMERGENCY OPERATIONS – ACTIVATION/ OPERATIONAL ASSIGNMENT UP TO 100% AT VARIOUS TIMES:

When requested to fill an operational assignment and until demobilized, the following duties will be performed and your regular duties may temporarily cease: 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.Staff need 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)If assigned on-call, standby or as a Duty Officer, 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.1. AFTER-HOURS: Employee may occasionally be contacted for after-hours emergency support.
2. TRAVEL: Employee is required to operate a State vehicle during the course of deployment as part of employment. Employee may be required to travel to respond to IR incidents at various sites within California.
3. TRAINING: Employee is required to successfully complete all training related to the functions of the job.
4. 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.**
5. **PHYSICAL: Employee will be working in a classified office environment. This** necessitates pulling open a metal vault door, which requires approximately 30 lbs. of pull to open the door for access.
6. OTHER: The position requires a valid California Drivers’ License (CDL).
 |
|  | Allocation Factors (Complete each of the following factors.)  |
|  | **Supervision Received:**The IT Spec II receives general direction from the Cal CSIC MSB Chief, ITM II, and functionally reports to and receives the majority of assignments from the Cal CSIC COB Chief, ITM II; however, direction and assignments may also come from a designated Team Lead.**Actions and Consequences:**Failure to effectively perform the duties of this position will result in the agency’s 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 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 Cal OES.**Personal Contacts:**This position will interact with all levels of staff including state agency Secretaries and departmental Directors, Agency Information Officers, Chief Information Officers, Information Security Officers, Privacy and Disaster Recovery Coordinators regarding cyber security issues, as well as, and stakeholders from other branches and levels of government, education, critical infrastructure sectors, National Associations, and private industry. Contacts typically have an objective requiring a common understanding of the problem and developing suitable solutions. **Administrative and Supervisory Responsibilities: (Indicate “None” if this is a non-supervisory position.)**The IT Spec II is responsible for monitoring project goals and objectives. **Supervision Exercised:**The IT Spec II does not supervise but may lead. 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 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. |
|  | **Desirable Qualifications: (List in order of importance.)** |
|  | CompTIA Security +, GIAC Security Essentials or equivalent certifications are desired.**Knowledge:*** 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 authentication, authorization, and access control methods.
* Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
* Knowledge of computer algorithms.
* Knowledge of encryption algorithms
* Knowledge of cryptography and cryptographic key management concepts
* Knowledge of database systems.
* Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
* Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
* Knowledge of incident response and handling methodologies.
* Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
* Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
* Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
* Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
* Knowledge of network traffic analysis methods.
* Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
* 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 policy-based and risk adaptive access controls.
* Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/ SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
* Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
* Knowledge of security system design tools, methods, and techniques.
* Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
* Knowledge of the cyber defense Service Provider reporting structure and processes within one’s own organization.
* Knowledge of Virtual Private Network (VPN) security.
* Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities.
* Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
* Knowledge of adversarial tactics, techniques, and procedures.
* Knowledge of network tools (e.g., ping, traceroute, nslookup)
* Knowledge of defense-in-depth principles and network security architecture.
* Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
* Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
* Knowledge of interpreted and compiled computer languages.
* Knowledge of collection management processes, capabilities, and limitations.
* Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
* Knowledge of cyber defense and information security policies, procedures, and regulations.
* Knowledge of the common attack vectors on the network layer.
* Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
* Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
* Knowledge of system administration, network, and operating system hardening techniques.
* Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
* Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
* 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 encryption methodologies.
* Knowledge of signature implementation impact for viruses, malware, and attacks.
* Knowledge of Windows/Unix ports and services.
* Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
* Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
* Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
* 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 systems security testing and evaluation methods.
* Knowledge of countermeasure design for identified security risks.
* Knowledge of network mapping and recreating network topologies.
* Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
* Knowledge of the use of sub-netting tools.
* Knowledge of operating system command-line tools.
* Knowledge of embedded systems.
* Knowledge of Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) tools and applications.
* Knowledge of network protocols such as TCP/ IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
* Knowledge of how to use network analysis tools to identify vulnerabilities.
* Knowledge of penetration testing principles, tools, and techniques.
* Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

**Skills:*** Skill in developing and deploying signatures.
* Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
* Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
* Skill in evaluating the adequacy of security designs.
* Skill in using incident handling methodologies.
* Skill in using protocol analyzers.
* Skill in collecting data from a variety of cyber defense resources.
* Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
* Skill in reading and interpreting signatures (e.g., snort).
* Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
* Skill in performing packet-level analysis.
* Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
* Skill in conducting trend analysis.
* Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
* Skill to use cyber defense Service Provider reporting structure and processes within one’s own organization.

**Abilities:*** Ability to analyze malware.
* Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
* Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
* Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
* Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
* Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
 |
| **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 |
| VACANT |  |   |
| **Supervisor Statement: I have discussed the duties of this position with the incumbent.**  |
| Supervisor Name (Print) | Supervisor Signature | Date |
| VACANT |  |   |