PROPOSED

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

RPA NUMBER (HR USE ONLY)
20-192

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 01/19/2021	B. APPOINTMENT EFFECTIVE DATE -	C. INCUMBENT NAME VACANT
D. CIVIL SERVICE CLASSIFICATION Information Technology Manager I (IT Mgr I)		E. POSITION WORKING TITLE IT Mgr I
F. CURRENT POSITION NUMBER 695-330-1405-005		G. PROPOSED POSITION NUMBER (Last three (3) digits assigned by HR) 695-331-1405-005
H. OFFICE / SECTION / UNIT / PHYSICAL LOCATION OF POSITION Office of Information Security (OIS)/ Security Operations Center (SOC)/ Security Solutions/ Rancho Cordova		I. SUPERVISOR NAME AND CLASSIFICATION John Cleveland, Information Technology Manager II (IT Mgr II)
J. WORK DAYS / WORK HOURS / WORK SHIFT (DAY, SWING, GRAVE) MONDAY – FRIDAY/ 8AM – 5PM/ 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 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 direction of the Security Operations Center (SOC) manager, Information Technology Manager II (IT Mgr II), the Information Technology Manager I (IT Mgr I) provides the technical and managerial guidance for the design and implementation of the ongoing development, maintenance, and support of production security systems and services managed by Security Solutions. The Information Technology Manager I (IT Mgr I) is a senior manager of the SOC who manages the California Department of Technology (CDT) Security Solutions Engineering and Administration groups. The IT Mgr I ensures the appropriate security monitoring, compliance and controls are established and operational for the computing and network services used by CDT and provided to CDT customers.

The IT Mgr I is responsible for working with technical subject matter experts, all management levels, which includes CDT, and other state entities to develop, implement, and maintain appropriate vulnerability assessments, remediation, and compliance as well as respond to security incidents. The IT Mgr I must develop and maintain expert level and current knowledge of relevant IT security infrastructure and technologies utilized by the SOC, knowledge of applicable State/ Federal and industry regulations and best practices with respect to information security, understanding of department and information security policies and procedures, and of vulnerability and threat management technologies, products, practices and processes. The IT Mgr I must develop and maintain expert level and current knowledge of the IT threat landscape, risk management processes and technologies, multiple operating systems, network architecture and protocols, a full picture of IT security technologies, as well as interoperability and interdependency of all of those and more. Security best practices and advanced complex technical and administrative requirements must be expertly interpreted and applied in a highly complex technical environment.

% of time performing duties

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

Oversee Security Solutions functional engineering and administration teams' tasks:

55%
-

- Develop strategy and manage Engineering and Administrative teams that design, implement, and maintain critical SOC technologies including but not limited to: Security Information and Event Management (SIEM) services, Security Orchestration, Automation and Response tools, cloud platforms, Continuous Integration and Continuous Delivery (CI/ CD), infrastructure as code development, endpoint protection technologies, intrusion detection and protection devices, host based protection technologies, 0-day and Advanced Persistent Threat (APT) technologies (sandboxing, behavioral monitoring, etc.), packet capture and metadata analytic systems, Data Loss Prevention (DLP) technologies, email hygiene systems, etc.

- In conjunction with the SOC manager, manage the development and implementation of playbook scripts that detail the steps to be taken for specific, indicated security events
- Apply expert level knowledge of indicators of compromise and threats to detect attacks or compromised assets including, but not limited to, threat tactics/ techniques/ procedures, in-depth knowledge of security network architecture, in-depth knowledge of IT platform operations (e.g. Windows, Linux, Advanced Interactive eXecutive [AIX], network devices), vulnerability exploits and management, methods of access and related controls, encryption technologies, etc.
- Produce reports as instructed or as needed to adequately reflect the operational status of security solutions utilized by the SOC, and the resources engaged.
- Participate in the procurement and engagement of outsourced security resources as needed.
- Maintain the highest level of expertise in security operations technologies, techniques and processes as well as threat actor techniques and operations.
- Develop and maintain an expert level of threat knowledge, malicious actor techniques, indicators or compromise, analytic techniques and methods, and SOC workflow processes.
- 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.
- Develop and maintain expert level knowledge of security best practices and regulatory requirements.
- Attend formal training and conferences as well as perform personal research of periodicals, journals, the Internet, etc. in order to develop and maintain mastery level knowledge.

Team Building

- Advocate team building; work cooperatively and collaboratively with other supervisors; ensure a positive climate for change; implement solution-oriented supervisor style that respects, encourages, includes, and promotes the interests of subordinate staff.
- Ensure all Security Solutions staff are trained in security incident response processes.
- Provide expert advice and high level/ complex technical expertise on system security software, controls, security practice, and Data Center security standards to CDT and statewide stakeholders.
- Direct the assurance processes for customer projects (server scanning, verification that new applications hosted at CDT meet security standards) prior to application production.
- Assist with the division's ongoing workload related to service desk tickets, change requests and other Information Technology Service Management (ITSM) processes.
- Participate in the development of and present complex material including position papers; budget change proposals.
- Encourage team building, facilitate cross training and promote continuous improvement. Use motivation techniques, provide training for employees, and create a positive climate for change.

Governance

- Assist in the development of the CDT information security policies, standards, and procedures reflecting new technology solutions and changes in CDT standards and/or processes.
- Direct reoccurring assessments and remediation efforts required to maintain system compliance with appropriate control sets and best practices.
- Assure adherence to CDT change control requirements and processes.
- Manage external engagement including scheduling, project management, and coordination with technical staff across CDT and customer departments to facilitate onboarding of logs and machine data.
- Manage technology evaluations, implementations, and administration.

20%

Participate in Security Operations activities as a threat and security subject matter expert.

- Participate in the development and maintenance of all necessary Security Operations policies, procedures, documents, and other artifacts as needed to operate and grow a successful security operations function.
- Represent Security Solutions Engineering and Administration groups as required in both internal and external meetings and engagements.
- Serve as the manager of staff in the investigation of system problems, tracking, resolution, and reporting to CDT management, oversight agencies, and customers as required.

% of time performing duties

- Participate in post-incident reviews to ensure that Security Operations tools are operating effectively and make modifications or enhancements as required.

20%

Supervise Security Solutions Engineering and Administration Staff working to support the SOC.

- Ensure Security Solutions staff are fulfilling their duties as described in their respective duty statements and as assigned.
- Responsible for completing Request Personnel Actions (RPAs) for various changes, promotions, out of class assignments or any other action impacting a position.
- Responsible for developing and updating duty statements for unit employees in conjunction with SOC management as needed establishing performance expectations.
- Complete Individual Development Plans (IDPs) annually, completing probationary reports in a timely manner, and other performance management activities including adherence to the State's progressive discipline policy including taking corrective action as necessary.
- Develop plans to accomplish unit goals and objectives in accordance with organizational mission and strategic plan.
- Ensure subordinate employees comply with all CDT policies, standard office operating procedures, and department and agency protocols.
- Foster methods of creative decision-making and problem solving and provide continuous feedback to employees.
- Provide technical and supervisory direction to staff in accordance with organizational mission and strategic plan.
- Review work-products, analytical studies, proposals, and correspondence.
- Responsible for staff changes, promotions, or any other action impacting a position.

5%

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

Represent Security Solutions as required at both internal and external meetings (e.g. customer meetings, the California Information Security Office (CISO), and other statewide workgroups). Keeping abreast of cybersecurity technologies and techniques, operating systems, network protection technologies, cloud services, system architecture, systems development lifecycle, and risk management. Develop and present complex material including: issue memos; position papers; budget change proposals, and feasibility study reports. Perform other related duties.

Work Environment Requirements

- The incumbent may be required to travel and may need to carry a mobile device.
- Must pass a fingerprint background check completed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI), and obtain Secret- level Clearance.

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

Supervision Received:

The incumbent works under general direction of the SOC IT Mgr II. The IT Mgr I is expected to direct and manage the completion of assignments by technical staff from general parameters, and is expected to prioritize workload and assignments within Security Solutions.

The incumbent is responsible for reporting progress, problems and changes in priority or schedules within Security Solutions and to CDT executive management as required. The incumbent is responsible for staff development and cross-training to ensure critical functions are staffed appropriately. The incumbent is required to operate with a high degree of independence in performing all duties

Actions and Consequences:

The incumbent is responsible for ensuring appropriate security controls are in place and enforced throughout CDT for all hosted applications and computing resources. The IT Mgr I 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 incumbent 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 Mgr I is in personal contact with a wide variety of technical, administrative and CDT executive staff on a daily basis. External contacts include CDT customers, CISO and senior management within customer departments.

Administrative and Supervisory Responsibilities: **(Indicate "None" if this is a non-supervisory position.)**
The IT Mgr I will advise the IT Mgr II in planning, budgeting, staffing, and operational activities of the SOC. The IT Mgr I will serve as part of the management team of the Security Monitoring and Intelligence (SMI) group helping to set the strategy and direction of that function as it expands and grows more complex. The incumbent will represent CDT Security Solutions at customer meetings and is expected to participate as required in statewide workgroups on security efforts within the state.

Supervision Exercised:
The IT Mgr I supervises Information Technology Specialists (ITSs) at various levels as assigned.

Other Information

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

- Ability to interpret and incorporate data from multiple tool sources
- Skill in supervising technical staff and accomplishing work through their and their staff's efforts
- Skill in collecting data from a variety of computer network defense resources
- Skill in conducting open source research for troubleshooting novel client-level problems
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
- Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs])
- Skill in data reduction
- Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)
- Skill in developing and deploying signatures
- Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode)
- Skill in network mapping and recreating network topologies
- Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- Skill in reading and interpreting signatures (e.g., Snort)
- Skill in reading Hexadecimal data
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks
- Skill in using incident handling methodologies
- Skill in using network analysis tools to identify vulnerabilities
- Skill in using protocol analyzers
- Skill in using sub-netting tools
- Skill in utilizing virtual networks for testing
- Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code),
- Knowledge of basic system administration, network, and operating system hardening techniques
- Knowledge of collection management processes, capabilities, and limitations
- Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities)
- Knowledge of common network tools (e.g., ping, traceroute, nslookup)
- Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities
- Knowledge of computer network defense (CND) policies, procedures, and regulations
- Knowledge of content development
- Knowledge of cryptology
- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
- Knowledge of defense-in-depth principles and network security architecture
- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution)

- Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])
- Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN])
- Knowledge of encryption methodologies
- Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)
- Knowledge of front-end collection systems, including network traffic collection, filtering, and selection
- Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)
- Knowledge of host/network access controls (e.g., access control list)
- Knowledge of how to troubleshoot basic systems and identify operating systems-related issues
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL])
- Knowledge of incident response and handling methodologies
- Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation
- Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies
- Knowledge of Intrusion Detection System (IDS) tools and applications
- Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])
- Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth)
- Knowledge of network traffic analysis methods
- Knowledge of new and emerging information technology (IT) and information security technologies
- Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit)
- Knowledge of policy-based and risk adaptive access controls
- Knowledge of programming language structures and logic
- Knowledge of security management
- Knowledge of signature implementation impact
- 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 the common attack vectors on the network layer
- Knowledge of the computer network defense (CND) service provider reporting structure and processes within one's own organization
- Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep)
- Knowledge of Virtual Private Network (VPN) security
- Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities
- Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat)

Knowledge of Windows/Unix ports and services

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
JOHN CLEVELAND		