**PROPOSED**

|  |  |
| --- | --- |
| State of CaliforniaCalifornia department of technologyDuty StatementTech 052 (Rev. 02/2018) | **RPA NUMBER (HR Use Only)** |
| **21-010**  |
| **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 9, 2021 |  | VACANT |
| d. CIVIL SERVICE CLASSIFICATION | e. POSITION WORKING TITLE |
| Information Technology Manager II | IT Mgr II |
| F. Current Position Number | G. proposed Position Number (Last three (3) digits assigned by HR) |
| 695- 331-1406-001 |  |
| H. office / section / unit / physical Location of Position | I. supervisor Name and classification |
| Office of Information Security/Security Operations Center / Rancho Cordova | John Cleveland, Deputy State Chief Information Security Officer, Security Operations |
| J. Work Days / Work Hours / work shift (day, swing, grave) | K. Position Requires:  | fingerprint background check | [x]  Yes [ ]  No |
| MONDAY – FRIDAY/ 8AM – 5PM/ DAY | 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[ ]  Software Engineering | [ ]  Client Services [x]  System Engineering |
|  | Organizational Setting and Major Functions |
|  | Under the administrative direction of the Deputy Director of Security Operations the InformationTechnology Manager II (IT Mgr II) serves as the California Department of Technology (CDT)Manager of Security Operations Center (MSOC). The MSOC is responsible for management andoversight of the CDT Security Operations Center which includes both Security Solutions andSecurity Monitoring and Intelligence (Security Operations Center [SOC]) groups. The MSOC ensures the monitoring and protection of Security Customers, which includes CDT and other state entities and participating customer information assets through the delivery of security services to those entities. This is accomplished through the development and implementation of the strategies, people, processes, and technologies necessary to accomplish that goal. The MSOC will be responsible for the development of the incident response practice and continuous improvement of the capabilities. Additionally, the MSOC interacts at all levels of executive and technical management within the state.  |
|  | **Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.)** |
| 40% of time performing duties20% of time performing duties10% of time performing duties10% of time performing duties10% of time performing duties5% of time performing duties | Security Operations Center and the associated organizations that secure business operations, and aligns with the states’ and CDT mission, goals, and objectives. The MSOC develops, implements,enforces, and maintains processes, practices, and (as needed) policies related to the InformationSecurity Operations Center. The MSOC ensures that the Information Security Operations Center is compliant with all applicable legal, statutory, regulatory, and best practice requirements. Withinthe purview of security operations people/process/technology triad, the Information SecurityOperations Center 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.

These objectives are accomplished through the Security Solutions group which provides and manages security technologies and services along with the Security Monitoring and Intelligence group which provides 24\*7 monitoring, detection, analysis, and response to security events within the SOC.Perform day-to-day management activities for Security Operations Center.* Develop plans to accomplish the Security Operations Center goals and objectives in accordance with organizational mission and strategic goal; support and advocate management’s philosophy, policies, and procedures.
* Evaluate supervisors on completion of their supervisory responsibilities; develop and update duty statements as needed, establish performance expectations, complete individual development plans annually, complete probationary reports on a timely basis, and other performance management activities including adherence to the State’s progressive disciplinary process and policy including taking corrective action as necessary.
* Implement informed and defensible administrative and personnel management decisions in accordance with department and state policies, personnel-related laws, rules, established CDT administrative processes and procedures, and collective bargaining agreements.
* Ensure the Security Operations Center supervisors comply with all applicable CDT policies, standard operating procedures, and department/agency protocols.
* Encourage team building, facilitate cross training and promote continuous improvement of processes. Implement motivation techniques, promote training, and create a positive climate for change.
* Foster methods of creative decision making and problem solving while providing continuous feedback to the Security Operations Center supervisors and staff.

**Process/Organizational Management:** Collaborate with CDT customer, executives and senior managers to integrate the requisite security technologies and processes into departmental processes, procedures, and technologies.**Security Architecture:** Collaborate with CDT, customers and partners information technologystaff, enterprise and security architects, and information security teams to ensure that the SecurityOperations Center technologies are consistent with, and supportive of, those initiatives and programs. Conduct maturity assessments to identify gaps and develop alternatives for investment recommendations to improve the affected CDT’s security posture in workforce, system and technical architecture, and business processes. Lead teams to research, evaluate, pilot, and implement new technologies for use in the Security Framework in support of enterprise and statewide business and surety initiatives. Define and publish the overall State Cloud security strategy with the consensus from operational and state Information Security Officer partners.**Strategic Planning:** Ensure the CDT Security Operations Center is in alignment with statewide information security initiatives while leading and participating in security planning and/or governance sessions. **Research and Innovation**: Research and evaluate current, and new, information security technology and trends to develop the Security Operations Center strategy and roadmap. |
|  | **Marginal Functions (Percentages shall be in increments of 5 and should be no more than 5%.)** |
| 5% of time performing duties | Support the CISO as required to represent the Office of Information Security both internally and externally. |
|  | **Work Environment Requirements*** The MSOC works in an office environment and is required to operate a personal computer, develop and analyze spreadsheets, conduct e-mail communications, develop presentations and diagramming applications, use technical software for monitoring a variety of security related items, as well as operate general office equipment to include, but not limited to the following; copy machine, fax machine, telephone system, etc.
* The MSOC is required to carry a mobile device, and may be required to travel when necessary.
* Must pass a fingerprint background check completed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI).

**Allocation Factors (Complete each of the following factors.)** **Supervision Received:**The IT Mgr II works under the administrative direction the Deputy Director of Security Operations. Assignments are given in general terms with the desired results and timeliness being specified. The IT Mgr II performs the various phases of the activity including the detail development and scheduling of tasks, progress review, problem identification, and changes in priority or schedules. The IT Mgr II is required to operate with an extreme degree of independence in performing all duties. **Actions and Consequences:**The IT Mgr II provides in-depth review and analysis of statewide data and network security standards and best practices. The IT Mgr II assists in developing and maintainingconfidentiality, integrity and availability to ensure compliance with the State AdministrativeManual and federal mandates. The IT Mgr II must use discretion while maintainingconfidentiality of all personal information, failure to successfully implement these responsibilitiescould result in severe consequences including the loss, or compromise of, critical data or StateIT assets.**Personal Contacts:**The IT Mgr II is in personal contact with a wide variety of departmental, Agency, and customer executive management, administrative and technical personnel, and vendor community on a daily basis.**Administrative and Supervisory Responsibilities: (Indicate “None” if this is a non-supervisory position.)**The IT Mgr II’s administrative duties include preparing status reports on assigned tasks, conducting presentations and meetings, authoring publications as needed, and performing research and analysis.**Supervision Exercised:**The IT Mgr II provides supervision to the lower level Information Technology Managers inSecurity Operations Center.**Desirable Qualifications:*** Experience in the management of a security program in a highly regulated industry.
* Experience in planning, improving, and implementing large, cross-functional, complex solutions.
* Experience in reporting on sensitive or critical risks and issues to executive management.
* Ability to build strategic relationships with industry partners in both the public and private sectors.
* Ability to develop and deliver strategic communications and security education programs.
* Ability to work collaboratively, and in partnership with, multiple agencies and localities that are or will be affected by the Security Operations function
* Experience in conducting assessments and implementing improvement plans.
* Experience in contract and vendor negotiations. Technical competence to lead organizations security operations initiatives, including knowledge of technical issues and the effect on business processes.
* Principles, practices, and trends of public administration, including management, organization, planning, cost/benefit analysis, budgeting, and project management and evaluation.
* Employee supervision, training, development and personnel management.
* Current computer industry technology and practices.
* Principles of data processing systems design, programming, operations, and controls.
* State level policies and procedures relating to EDP.
* The department’s goals and policies.
* Department’s Equal Employment Opportunity (EEO) objectives.
* A manager’s role in the Equal Employment Opportunity Program and the processes available to meet EEO.
* Effectively contribute to the department’s EEO objectives.
* Principles of the governmental functions and organizations at the State level, including the legislative process.

Ability to:* Develop and evaluate alternatives, make decisions and take appropriate action.
* Establish and maintain priorities.
* Effectively develop and use resources.
* Identify the need for and assure the establishment of appropriate administrative procedures.
* Plan, coordinate and direct the activities of a data processing staff.
* Make effective use of interdisciplinary teams.
* Reason logically and creatively and use a variety of analytical techniques to resolve managerial problems.
* Present ideas and information effectively, both orally and in writing.
* Consult with and advise administrators and other interested parties on a variety of subject matter area, translating technical data processing terms into everyday language.
* Gain and maintain the confidence and cooperation of others.
 |
|  |  |

|  |
| --- |
| **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 |
|   |  |   |