|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| State of California  California department of technology  Duty Statement PROPOSED  Tech 052 (Rev. 02/2018) | | | | | | **RPA NUMBER (HR Use Only)** | | | |
| **23-002** | | | |
| **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 | | | | | |
| 7/7/2023 | |  | | VACANT | | | | | |
| d. CIVIL SERVICE CLASSIFICATION | | | | e. POSITION WORKING TITLE | | | | | |
| IT Manager II | | | | Senior Advisor to State CISO and Deputy CISO | | | | | |
| F. Current Position Number | | | | G. proposed Position Number (Last three (3) digits assigned by HR) | | | | | |
| 695-405-1406-002 | | | |  | | | | | |
| H. office / section / unit / physical Location of Position | | | | I. supervisor Name and classification | | | | | |
| Office of Information Security/ Rancho Cordova | | | | John Cleveland, OIS, Deputy Chief ISO, CEA C | | | | | |
| J. Work Days / Work Hours / work shift (day, swing, grave) | | | | K. Position Requires: | fingerprint background check | | | | Yes  No |
| MONDAY-FRIDAY 8AM – 5PM/ DAY | | | | 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  Information Security Engineering | | | IT Project Management  Software Engineering | | | Client Services  System Engineering | | |
|  | Organizational Setting and Major Functions | | | | | | | | |
|  | Under the administrative direction of the Deputy Chief Information Security Officer (CISO), the Information Technology Manager II (IT Mgr II) has significant responsibilities that impacts State enterprise-wide information security programs at both the Agency and entity level. The IT Mgr II advises the CISO and the Deputy CISO on the formulation of policy and governance and has a significant role in developing cybersecurity strategy and strategy implementation. The incumbent is responsible for, partnership with Office of Information Security (OIS) managers, delivering the OIS Project Portfolio major projects and initiatives. | | | | | | | | |
|  | Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.) | | | | | | | | |
| % of time performing duties  30%  20%  20%  20%  5%  5% | Leads the implementation of Cal-Secure, the State of California’s on-going Statewide strategic planning, privacy and cybersecurity strategy.   * Responsible for the implementation of Cal-Secure workforce priorities and initiatives through partnerships with agencies, state entities and external partners. This includes the development of job roles, categories and knowledge skills using the National Initiative for Cybersecurity Education (NICE) framework, increasing sources of cybersecurity talent through partnerships and expanding cybersecurity training opportunities for state staff and leadership. * Oversight and overall management of the 15 initiatives within Cal-Secure. Provides leadership and strategic direction to OIS project teams to ensure Cal-Secure objectives are accomplished. Reviews and approves the master project plan and schedules. Works with Agency Information Security Officers to ensure that Agency-level strategic plans are developed and aligned with the CalSecure areas of People, Process, and Technology.   Provides Statewide communications, leadership and oversight of the OIS Project Portfolio of major projects and initiatives.   * Oversight and management of the OIS Project Portfolio through the development and execution of centralized tracking and project portfolio best practices. Ensure strategic alignment and prioritization of all projects and initiatives. Report on issues impacting resource management, planning and scheduling and in collaboration with OIS managers work to resolve issues. Supports, revises and maintains OIS alignment to all Bridge to Future efforts, as well as all subsequent strategic planning. * Project sponsor for enterprise-wide projects. Act as project sponsor and provide leadership and direction to the Unified Integrated Risk Management Project (an enterprise project impacting all state agencies and entities) to ensure project and organizational objectives are accomplished via effective project management and that all stages of the Project Approval Lifecycle (PAL) are completed in accordance with SIMM 19. Plan, direct and oversee the project ensuring that deliverables and functionality are achieved as defined in the project charter, funding documentation and subsequent plans. Ensure that mission critical program requirements are properly addressed. Negotiate with senior stakeholders and decision makers on issues of critical importance to the project’s success. Develop Budget Change Proposal (BCP) to support the project. * Oversight and overall management of all efforts associated with zero trust architecture, including policy and standards development, reference architecture development and adoption, and reporting.   Direct and coordinate with the California Military Department and OIS Audit team to develop and maintain annual Independent Security Assessment (ISA) and Information Security Program Audit (ISPA) schedules and resolve conflicts with state entities. Incumbent also analyzes requests for 3rd party assessments to ensure standards would be met if approved.  Planning and coordinating fiscal resources between OIS internal and external units and departments   * Manage all Budget Change Proposals (BCPs) * Provide Project Approval Lifecycle Critical Partner (PAL) reviews and recommendations throughout the year. * Coordinate and deliver responses on behalf of OIS. * Manage all legislative analysis related to cybersecurity and privacy on behalf of OIS and coordinate all responses including fiscal analysis and BCP requests spawned from proposed legislation.   Independently advise executive level (CISO and Deputy Director) on cybersecurity strategy, policy and governance to ensure current and future enterprise and organization requirements are met.  Act as the Program Coach for the Information Security Leadership Academy (ISLA). Work directly with CDT Office of Professional Development annually to develop and/or modify curriculum. Manage the class program throughout the ISLA session. | | | | | | | | |
|  | Marginal Functions (Percentages shall be in increments of 5, and should be no more than 5%.) | | | | | | | | |
|  | N/A | | | | | | | | |
|  | Work Environment Requirements | | | | | | | | |
|  | * Professional office environment, business dress, according to current office policy; * Must pass a security background check and fingerprinting check completed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) as a condition of employment with the Office of Information Security. * This position requires the ability to work excess hours, to effectively handle stress while working under pressure to meet deadlines and the ability to travel to meetings. | | | | | | | | |
|  | Allocation Factors (Complete each of the following factors.) | | | | | | | | |
|  | **Supervision Received:**  The IT Mgr II receives administrative direction from the Deputy CISO.  **Actions and Consequences:**  The IT Mgr II is responsible for enterprise-wide cybersecurity strategy development and implementation, project portfolio management and execution and significant reportable projects. The consequence of error is increased security risk exposure and liability for the state.  **Personal Contacts:**  The IT Mgr II will have regular contact with CDT executives, Agency Information Security Officers, Agency Information Officers, the Department of Finance, California Department of Human Resources, California Government Operations Agency and external partners.  **Administrative and Supervisory Responsibilities: (Indicate “None” if this is a non-supervisory position.)**  The IT Mgr II has administrative responsibilities over projects within the OIS Project Portfolio including the implementation of Cal-Secure. The incumbent represents CDT and OIS at customer, vendor and partner meetings, and is expected to participate in statewide workgroups on the security efforts within the state.  **Supervision Exercised:**  The IT Mgr II directly manages project managers associated with project portfolio projects. | | | | | | | | |
|  | Other Information | | | | | | | | |
|  |  | | | | | | | | |
|  | **Desirable Qualifications: (List in order of importance.)** | | | | | | | | |
|  | * IT and information security experience working at a senior level exercising a high degree of initiative and independence of action with senior management and stakeholders. * Experience developing enterprise level information technology and/or cybersecurity strategies, impact statements, cost/benefit analysis and roadmaps. * Experience working at a senior level, including the development of strategies and management of enterprise-wide projects. * Experience advising senior management on strategy, policy and governance. * Thorough understanding of the principles, practices, and trends related to information security and information technology. * Thorough knowledge of project, contract, and vendor management methodologies and best practices. * Experience with the State’s administrative process, including experience in BCP development, HR functions, Legislative bill analysis and program management. * Ability to establish and maintain effective, cooperative and beneficial relationships on behalf of CDT with all levels of government, control agencies, stakeholders, external customers and vendors. * Ability to effectively plan project assignments, allocate resources and adapt easily to change priorities. * Knowledge of the principles, practices, and trends of public and business administration, including management, organization, planning, cost/benefit analysis, budgeting, project management and evaluation; employee supervision, training, development and personnel management. * Strong written, verbal and communications and negotiating skills. * Proven track record of gaining confidence and trust of individuals in key positions. | | | | | | | | |
| **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 | |
| John Cleveland, Deputy State CISO | | |  | | | | |  | |