|  |  |
| --- | --- |
| State of CaliforniaCalifornia department of technologyDuty Statement PROPOSEDTech 052 (Rev. 02/2018) | **RPA NUMBER (HR Use Only)** |
|  **23-076** |
| **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 |
| 10/4/2023 |  |  |
| d. CIVIL SERVICE CLASSIFICATION | e. POSITION WORKING TITLE |
| Information Technology Manager I  |  Advisory Services Program Manager |
| F. Current Position Number | G. proposed Position Number (Last three (3) digits assigned by HR) |
|  695-405-1405-015  |   |
| H. office / section / unit / physical Location of Position | I. supervisor Name and classification |
|  Office of Information Security/Advisory Services Program/Infusion Team/Rancho Cordova  | John Hanafee, Information Technology Manager II  |
| J. Work Days / Work Hours / work shift (day, swing, grave) | K. Position Requires:  | fingerprint background check | [x]  Yes [ ]  No |
|  MONDAY-FRIDAY 8:00 A.M. TO 5:00 P.M.  | 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.)** |
| [x]  Business Technology Management[x]  Information Security Engineering | [ ]  IT Project Management[ ]  Software Engineering | [ ]  Client Services [ ]  System Engineering |
|  | Organizational Setting and Major Functions |
|  | Under the general direction of the Information Technology Manager II (IT Mgr II), the Information Technology Manager I (IT Mgr I) in Advisory Services Program (ASP) serves as the program manager in the delivery of Advisory Services. The IT Mgr I oversees ASP’s special programs administration and other activities designed to assist state agencies/departments with their information security programs. The IT Mgr I is responsible for the administration of the vCISO and ASP Infusion Team/program. Supervise the work of the vCISO contract and the staff assigned to the Infusion Team, comprised of IT Specialist II positions. The incumbent is responsible for the planning and execution of pre-audit and post-audit workshops, The incumbent is responsible for planning and supporting the Office of Information Security (OIS) Advisory Services Program (ASP) security program strategies to Agency Information Security Officer (AISO) and Information Security Officer (ISO) within state entities; the development and tracking of risk remediation plans, managing and overseeing security solutions for highly complex technical problems, implementation of technical system and procedures for addressing security gaps, the development and maintenance of a portfolio of required policy templates, security artifacts and tools utilized by the statewide ISO community; the development and delivery of security-related workshops; and OIS outreach.  |
| % of timeperforming duties | Essential Functions (Percentages shall be in increments of 5 and should be no less than 5%.) |

|  |  |  |
| --- | --- | --- |
| **40%**% of timeperforming duties**25%****10%****10%****10%** |

|  |
| --- |
| **vCISO and Infusion Programs Administration*** Supervise Infusion Team staff working to support the ASP and state community. Develop and oversee the ASP Infusion program. Research, develop, maintain risk management profiles for CISO/ISOs within departments. Administrate agreements for services, develop statement of work, evaluate deliverables and build, allocate, maintain, and track criteria for department participation and allocation of resources. Lead budget, staffing, and contracting. Establish and track milestones and metrics for performance. Write and present reporting metrics and program status to senior OIS management on a periodic basis.
	+ Ensure the Infusion Team staff fulfil their duties as described in their respective duty statements 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 security operations 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.
	+ 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.

**Oversee virtual CISO (vCISO) program.** * Administrate contracts for services, develop statement of work, and procurement materials. Build criteria for department participation and allocation of resources. Lead and oversee budget, staffing, and contracting. Establish and track milestones and metrics for performance. Write and present program metrics to senior OIS management on a periodic basis.

**Plan, schedule, conduct and manage pre-audit and post-audit workshops and post ISA workshops for the most complex organizations.** * Develop a customized pre-audit workshop plan for the most complex departments utilizing the standard workshop framework and customized using relevant department security artifacts. Develop a daily plan-of-action and schedule for each workshop, customized by department needs.
* Identify, plan, and communicate the workshop scope, objectives, approach, timing, and deliverables to affected parties.
* Lead the workshop and document the progress and results. Create a pre-audit workshop plan and post-audit workshop report for each department.
* Plan post-audit workshop utilizing the results of the OIS security audit or ISA as the starting point.
* Develop a customized post-audit or post ISA workshop, which includes a review of findings, consulting on best practices approach and standard tools and templates.

**Training*** Produce workshops annually utilizing subject-matter-experts that address specific needs of the ISO community and are tailored to the state environment.
* Produce the ISO training courses. Ensure that Subject Matter Expert (SME) presentations and all preparations are timely.
* Conduct training surveys post-workshops and periodically with the ISO community to ensure that OIS provided training and workshops are aligned with meetings.
* Coordinate with the CDT Deputy Director – Office of Professional Development on the training needs of the ISO community.

**Operations*** Contribute, maintain, and update the ASP operational procedures and artifacts. Document ASP processes and ensure accuracy and compliance with all relevant office policy and procedures and alignment with audit team manual.
 |

 |
|  | Marginal Functions (Percentages shall be in increments of 5 and should be no more than 5%.) |
| **5%** | Assist with other statewide program representation, training, and related activities. Specific duties may include: * Make presentations at ISO, Information Security Advisor Council (ISAC) meetings, to senior department management and to the CDT Directorate.
* Conduct outreach to the ISO community to ensure Advisory Services is aligned with ISO community needs.
* Contribute as a member of the OIS Audit Change Control Board.
* Contribute to the creation, update, maintenance and retirement of templates, forms and artifacts that includes the required community input and CISO approval of action.
* Create, update, maintain, and retire templates, forms and artifacts that meets the needs of the ISO community and that assist them in meeting mandated requirements for their security programs.
* Assist the ASP Template Coordinator
 |
|  | Work Environment Requirements |
|  | * Incumbent will be required to support a work from home environment. Incumbent is expected to maintain a secure workspace within their home and support necessary logistical requirements to support remote video conferencing and remote work. All work materials must be maintained in a secure environment.
* 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 handle stress while working under pressure to meet deadlines, use of a computer to communicate and prepare written materials, and the ability to travel to meetings, pre-audit workshops, post-audit workshops, and training locations.
* 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 I receives general direction from the IT Mgr II. **Actions and Consequences:**The IT Mgr I is required to have knowledge of Government Accountability Office's Generally Accepted Government Auditing Standards, and the American Institute of Certified Public Accountant's Statements on Auditing Standards, and Information Systems Security Audit and Assurance Standards, NIST Risk Management Framework and NIST/FIPS Standards. This program has a significant statewide impact and is part of the overall California information security program. The consequences of error, lack of knowledge of audit standards and accuracy results in increased security risk exposure and liability for the state. **Personal Contacts:**This position will interact with all levels of staff including (state agency and departmental Agency Directors), Agency Information Officers, Chief Information Officers, Information Security Officers, Privacy and Disaster Recovery Coordinators, and stakeholders from other branches and levels of government. **Administrative and Supervisory Responsibilities: ( Indicate “None” if this is a non-supervisory position.)**Manages all aspects of the pre-audit, post-audit, and post-ISA workshops, IT specialist staff supervision of special programs, preparing status reports on assigned tasks, conducting presentations and meetings, authoring publications as needed, and performing research and analysis. **Supervision Exercised:**The IT Mgr I manages staff within the Advisory Service Program vCISO & Infusion Team business unit. |
|  | Other Information |
|  |  This position requires significant communications with all levels of state government. Additionally, the incumbent will conduct workshops and training and therefore must have excellent writing, speaking and communication skills.   |
|  | **Desirable Qualifications:**  |
|  | * Knowledge of federal and state information security policies, standards, principles, practices, and frameworks such as Chapter 5300 of the State Administrative Manual and NIST Special Publication 800-53 and other 800-series publications, FIPS 140,199 & 200.
* At least two years of experience performing audits in the field of information technology.
* Extensive knowledge of federal and state information security policies, standards, principles, practices, and frameworks.
* Excellent verbal and written communication skills, including the ability to prepare presentations, reports, and other types of documentation at short notice. Ability to develop and maintain effective and cooperative working relationships.
* Ability to present information effectively to staff at all levels and from a wide variety of state entities to prepare entities for audit activities.
* Ability to communicate effectively with senior and executive management to convey results of Advisory Services efforts and initiatives as well as individual entity results.
* Ability to exercise a high degree of initiative and independence of action, with state entities and various stakeholders.
* Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.
* Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
* Skill in applying confidentiality, integrity, and availability principles.
* 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 identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.
* Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
* Knowledge of business continuity and disaster recovery continuity of operations plans.
* Knowledge of controls related to the use, processing, storage, and transmission of data.
* Knowledge of Application Security Risks (e.g., Open Web Application Security Project Top 10 list)
* The incumbent has obtained and continuously maintains one or more of the following certifications in information security: Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA), GIAC Security Expert (GSE).
 |
| **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 |
|  |  |   |