State of California
High-Speed Rail Authority

Job Description

Position Details

Classification: Information Technology Manager II

Office/Branch: Information Technology/Information Security Services

Working Title: Chief Information Security Officer

Location: Sacramento

Position Number: 311-420-1406-003

HR Approval Date/Initials: JT 5/23/24

CBID/Bargaining Unit: M01

Work Week Group: E

Tenure: Permanent

Time Base: Full Time

Job Description Summary

Under the administrative direction of the Chief Information Officer (CIO), the Information Technology (IT) Manager II serves as the Chief Information Security Officer (CISO) and is responsible for the Authority's Information Security program, including the direction, oversight, and operations of the IT Security Office and Privacy program. In addition, the CISO is responsible for establishing and overseeing the Operational Technology (OT) Cybersecurity Program for high-speed rail operations.

Directly and through subordinate management, the incumbent establishes the information security architecture; implements policies and procedures to maintain, monitor, control, and protect the Authority's information assets; assesses systems and processes to ensure compliance; and monitors and directs the mitigation of risks and vulnerabilities.

The following IT Domains are applicable to the incumbent's duties/tasks:

☒ Business Technology Management
☒ Client Services
☒ Information Security Engineering
☒ Information Technology Project Management
☐ Software Engineering
☒ System Engineering

Duties

Percentage
Essential (E)/Marginal (M)

35% (E) **Chief Information Security Officer (CISO)**

- Collaborates with the CIO and other IT Leadership in the development of technical roadmaps, enterprise architecture standards, and strategies to best align technology solutions with business and organizational needs. Participates in IT and Data Governance committees and groups and provides recommendations

ADA Notice: For individuals with sensory disabilities, this document is available in alternate formats. For information, please call the EEO Officer at (916) 324-1541, email at eeo@hsr.ca.gov, or write to: California High-Speed Rail Authority, at 770 L Street, Suite 620, Sacramento, CA 95814 and guidance to ensure compliance with Authority, State, and Federal policies and standards.

- Oversees all security audit and assessment work and directs necessary improvements.
- Oversees regular security reviews that audit all major systems and data processing activities to ensure compliance with laws, regulations, and Authority policies.
- Monitors compliance to and oversees the development and ongoing review of security policies, standards, and procedures.
- Monitors and analyzes emerging technology risks and develops and implements plans for mitigation.
- Oversees the development, implementation, and ongoing review of a strategic and comprehensive privacy program.
- Ensures the Plan of Action Milestones (POAM), Risk Management and Privacy Compliance, Technology Recovery Plan, and other plans or reports deemed necessary are developed, updated, and submitted to control agencies as required.
- Oversees and monitors the management and operation of various security tools such as endpoint security solutions, vulnerability scanners, Identity and Access Management systems, Managed Security Service Provider (MSSP), etc.
- Oversees the identification, ownership, and classification for all systems, records, files, and databases to ensure the integrity and security of agency information assets.
- Ensures information security and privacy awareness and education programs are implemented and maintained; supports actions taken for non-conformance.
- Maintains knowledge of Information Security trends, best practices, and emerging technologies and direct continuous improvement of security services in compliance with the SIMM 5300, Security Framework.
- Coordinates and collaborates with senior and executive-level leadership within and external to the Authority, control agencies, and other state and federal entities.

35% (E) **Operational Technology (OT) Cybersecurity**

- Establishes OT cybersecurity policies and procedures and implements processes to assess standards and requirements.
- Conducts and coordinates incident responses and ensures physical security controls on critical infrastructure.
- Establishes cybersecurity training and awareness programs for all personnel working on, with, or around OT control systems; and evaluates efficacy and compliance.

- Collaborates with rail system engineers, control system providers, operators, and other subject matter experts to integrate cybersecurity processes into the OT engineering and operations lifecycle.
- Identifies and oversees the application of technologies that reduce, mitigate, and/or automate cybersecurity functions such as Asset Management, Penetration Testing, Configuration and Patch Management, Cybersecurity Monitoring, Incident Response, Case Management, and System Restoration or Recovery.
- Monitors and provides input and guidance during the planning and implementation of rail system OT and the IT/OT convergence to ensure specialized security controls are implemented to ensure systems are protected against cyberthreats.
- Reviews and provides input to rail systems procurements and task orders for awarded contracts and reviews deliverables for compliance to requirements.
- Establishes a Security Information and Event Management (SIEM) system to provide real-time visibility across OT security systems. Integrates with, where appropriate, IT systems.
- Establishes a Security Orchestration, Automation, and Response (SOAR) platform to respond to alerts provided by the SIEM.
- Establishes new or expands existing security programs (i.e., Data Loss Prevention, Incident Response, Application Security, Vulnerability, etc.) to ensure the safety and security of OT systems, information, and data.
- Performs independent research; attends forums or workshops or other events, and collaborates with rail system engineers, operators, and external subject matter experts to gain knowledge and understanding of relevant control systems to inform all aspects of the OT Cybersecurity Program.
- Ensures compliance with all security policies, controls, protocols, and frameworks such as the Federal Information Security Modernization Act (FISMA), the National Institute of Standards and Technologies (NIST), and ISO 27001.

25% (E) **Leadership and Administration**

- Serves as a member of the IT Leadership team; participates in the development of IT policy and direction; communicates direction, strategy, and operational decisions to subordinate staff; and ensures adoption and conformance.
- Provides direction, guidance, and leadership to subordinate managers, staff, and contracted personnel on the implementation, and ongoing operations of the Information Security and OT Cybersecurity Programs.
- Identifies opportunities for and implement improvements, and monitors conformance and success.
- Identifies, documents, and communicates performance expectations; conducts regular team and one on one meetings; conveys expectations via written and verbal communication/direction; provides opportunities for continuous learning; and appraises job results.
- Identifies, documents, and communicates performance or conformance issues; holds staff accountable; develops or monitors improvement plans; and provides opportunities for continuous learning and professional growth.
- Contributes to workforce planning, budgeting, and succession planning.
- Supports IT and Data Governance programs and plans, and actively participates in governance programs and committees.

5% (E) **Other Duties**

- Collaborates with peers and provides support for initiatives across all areas of the IT Office.
- Represents the IT Office in meetings with Authority management, staff, and external partners and entities.
- Represents the Authority in meetings, workshops, or forums related to technology direction and planning.
- Fosters an environment of teamwork and collaboration and recognizes and communicates individual and team accomplishments.
- Actively participates in team and departmental meetings, training, technology initiatives, or other assignments.
- Maintains up to date knowledge about state policies, processes, and industry best practices related to IT administration.
- Ensures travel is approved and documentation and expense claims are processed in a timely manner.
- Invests in personal development through continuous education to gain and enhance position-related knowledge.

- Adheres to Authority policies and procedures regarding attendance, leave, and conduct.
- Other duties as needed to accomplish the Authority and IT Office's mission and goals.

Special Requirements

The checked boxes below indicate any additional requirements of this position.

License Required	Conflict of Interest (COI)	Bilingual Required	Contract Manager	Medical Required
Yes ☐ No ☒ Type:	Yes ☒ No ☐	Yes ☐ No ☒ Language:	Yes ☒ No ☐	Yes ☐ No ☒

Other Special Requirements Information:

- **Conflict of Interest (COI) –** This position is designated under the Conflict-of-Interest Code. The position is responsible for making, or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The employee is required to complete form 700 within 30 days of assuming employment. Failure to comply with the Conflict-of-Interest Code requirements may result in disciplinary action.

- **Contract Manager –** Ensures that assigned contracts and agreements are administered and managed in accordance with the applicable policies and procedures of the Authority, the State Contracting Manual (SCM), and the California Government Code (GC).

- **Manager of Contract Managers –** Provides strong oversight of subordinate contract managers, holding them accountable for ensuring that assigned contracts and agreements are administered and managed in accordance with the applicable policies and procedures of the Authority, the State Contracting Manual (SCM) and the California Government Code (GC).

Knowledge and Abilities

All knowledge and abilities for all Information Technology classifications; and

Ability to: Manage through subordinate supervisors; effectively promote equal opportunity in employment and maintain a work environment which is free of discrimination and harassment; and effectively contribute to the department's Equal Opportunity objectives.

Desirable Qualifications

- Bachelor's degree in an information technology related field of study.
- 5 years of related experience in information security or equivalent combination of education and experience.
- Possession of one or more of the following active certifications is desirable:
  - CompTIA Security+
  - Certified Cloud Security Professional (CCSP)
  - Certified Information Security Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
  - GIAC Continuous Monitoring Certification (GMON)
- Demonstrate comprehensive understanding of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, California State Administrative Manual (SAM), and California Statewide Information Management Manual (SIMM).
- Knowledge of information security incident response processes and procedures.
- Working knowledge of cloud computing platforms such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud.
- Knowledge of security devices such as network firewalls, web application firewalls, web content filters, and intrusion prevention/detection systems.
- Knowledge of networking concepts and practices.
- Knowledge of industrial control systems, OT engineering and operations lifecycle.
- Knowledge of project management practices, the system development lifecycle, etc.
- Ability to independently research and exhibit enthusiasm for continuous learning; ability to apply knowledge to inform decisions and direction.
- Exhibit a talent and passion for information security; is creative and resourceful in solving problems to meet business needs and demonstrate a service oriented, customer relations-sensitive attitude.
- Ability to establish and maintain cooperative working relationships with all levels of staff and management, and communicate effectively with peers, other technical teams, executives, external partners, vendors, and others.
- Ability to manage multiple high priority initiatives in a fast-paced achievement-oriented environment and work under pressure to meet deadlines.
- Ability to maintain confidentiality of sensitive tasks, assignments, and information.
- Ability to prepare and produce clear and concise documentation (e.g., processes and procedures, plans, information security policies, etc.).
- Willingness to work excess hours to achieve business results.

Supervision Exercised Over Others

This position supervises subordinate staff in the Information Technology Manager I, Information Technology Specialist II, and Information Technology Specialist I classifications. Provides general administrative direction concerning assignments.

Public and Internal Contacts

The incumbent will have regular contact with various levels of staff at the Authority, consultants, vendors, contractors, control agencies, and staff at other state agencies. The incumbent must handle all situations and communications tactfully and respectfully to support the Authority's mission.

Responsibility for Decisions and Consequence of Error

The employee has broad management responsibility for a large program or set of related functions. Administrative direction is usually received in terms of goals, and review is received in terms of results. At the Manager II level, incumbents are responsible for independent work within business constraints. This level is responsible for the recommendations to executives, decisions for projects, and outputs. This level is also responsible for program, project, and staff decisions and actions. The consequence of error at the Manager II level may have statewide and enterprise-wide impacts. Consequences include lost funding, project failure, failed business strategy, poor customer service and performance, risk exposure, loss of business continuity, missed business opportunities, and budget implications.

Physical and Environmental Demands

While working on-site, the incumbent works in a professional office environment, in a climate-controlled area which may fluctuate in temperature and is under artificial light. The incumbent will be required to use a computer, mouse, and keyboard, and will be required to sit for long periods of time at a computer screen. The incumbent must be able to focus for long periods of time, multi-task, adapt to changes in priorities, and complete tasks or projects with short notice. The incumbent must develop and maintain cooperative working relationships and display professionalism and respect for others in all contact opportunities.

Working Conditions and Requirements

a. Schedule: Flexible schedules may be available for this position.
b. Telework: Telework is available for this position with a minimum of two in-person working days per week.
c. Travel: Travel may be occasionally required domestically or internationally to support continuous education or to partner with system providers, operators, and other subject matter experts.
d. Other: The incumbent will be required to carry a state-issued cell phone and work outside of their regular schedule, as needed, to meet business needs.

Acknowledgment and Signatures

I have read and understand the duties listed above and can perform them with/without reasonable accommodation (RA). (If you believe you may require RA, please discuss this with the supervisor indicated below who will discuss your concerns with the RA coordinator. If you are unsure whether you require reasonable accommodation, inform the supervisor indicated below who will discuss your concerns with the RA Coordinator.)

Employee Printed Name:	Signature:	Date:

I have discussed the duties with and provided a copy of this duty statement to the employee named above.

Supervisor Printed Name:	Signature:	Date:

ADA Notice: For individuals with sensory disabilities, this document is available in alternate formats. For information, please call the EEO Officer at (916) 324-1541, email at eeo@hsr.ca.gov, or write to: California High-Speed Rail Authority, at 770 L Street, Suite 620, Sacramento, CA 95814