State of California
High-Speed Rail Authority

Job Description

Position Details

Classification:
Information Technology Specialist II

Office/Branch: Information Technology/Information Security Services

Working Title: Information Security Specialist

Location: Sacramento

Position Number: 311-420-1414-003

HR Approval Date/Initials: 2/10/25 MP

CBID/Bargaining Unit:	Work Week Group:	Tenure:	Time Base:
R01	E	Permanent	Full-time

Job Description Summary

Under general direction of the Security Operations Manager, an Information Technology (IT) Manager I, the IT Specialist II (Information Security Specialist) works independently and as part of a team to implement, maintain, and/or oversee the Enterprise Vulnerability Management Program, perform penetration testing, and monitor the Authority's Security Information Event Management (SIEM) system. The incumbent also leads the implementation of Zero Trust principles.

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)

30% (E) **Enterprise Vulnerability Management**

- Manages, maintains, and oversees the enterprise vulnerability management program for all servers, workstations, and other devices.
- Conducts threat and vulnerability assessments.
- Performs vulnerability scans to identify vulnerabilities and prioritizes the remediation of vulnerabilities across the enterprise according to level of risk to the Authority's information assets; creates plans of action to address the prioritized vulnerabilities throughout the enterprise.
- Establishes and maintains routine reports and real-time dashboards to display and report on the status of vulnerabilities across the enterprise.

- Monitors hardware and software vendor notifications for security vulnerabilities, and critical system and software updates.
- Performs research and provides technical guidance and recommendations regarding security enhancements to systems and applications.
- Reviews system change requests and procurements and participated on project teams to ensure the potential of security and operational risks and impacts are minimized or mitigated.
- Participates in Change Control Board (CCB) meetings and processes to ensure updates and patches are tested and implemented in accordance with the sensitivity or urgency of an identified vulnerability.
- Collaborates with IT staff and management, external partners, and solution providers to ensure vulnerabilities are identified and mitigated within established service levels.
- Contributes to the maintenance and accuracy of the Authority's hardware and software standards and inventory.
- Contributes to Technology Recovery Plan (TRP) development and updates and risk assessments; participates in recovery tests, such as tabletop exercises.
- Stays abreast of current cybersecurity threats that may affect Authority information assets.

20% (E) **Penetration Testing**

- Develops, plans, and executes effective penetration tests on systems, networks, applications, and devices to identify vulnerabilities and security issues.
- Performs vulnerability assessments on a regular basis, using both automated tools and manual techniques, to identify vulnerabilities and security threats.
- Reports on and presents all aspects of penetration tests, including vulnerabilities discovered, attack techniques utilized, and evidence gathered.
- Conducts follow-up vulnerability assessments and testing to verify that vulnerabilities have been effectively addressed.
- Creates and refines penetration testing methods to ensure the ongoing effectiveness of the penetration testing framework and program.
- Conducts and delivers presentations and training sessions on penetration testing techniques, tools, and best practices with relevant IT personnel.
- Ensures that all penetration testing activities are compliant with organizational and regulatory standards.

20% (E) **Security Information and Event Management (SIEM)**

- Manages, monitors, and/or oversees SIEM systems and third parties engaged in event monitoring.
- Develops and refines detection rules to improve SIEM's ability to identify specific threats and reduce false positives.
- Analyzes and validates security events/alerts from different data sources to identify potential threats, anomalies, and patterns indicative of security incidents.
- Monitors security events in real-time to detect suspicious activity, unauthorized access, or security breaches as they occur; takes appropriate action in response to real and potential threats.
- Responds to alerts based on predefined security thresholds, notifying security teams, asset custodians, and relevant stakeholders of potential incidents that require further investigation.
- Ensures SIEM systems are configured to meet compliance requirements (e.g., PCI-DSS, HIPAA, GDPR) and generates reports for auditing and regulatory purposes.
- Establishes and maintains Log Retention and Management to ensure logs are retained according to legal, regulatory, and organizational requirements and efficiently managed for analysis or compliance checks
- Participates or leads incident management or response teams, as appropriate.

20% (E) **Network Security – Zero Trust**

- Leads the implementation of Zero Trust principles across the organization's network, applications, endpoints, and cloud environments.
- Conducts a thorough analysis of the organization's existing security posture to identify gaps and opportunities for the Zero Trust framework.
- Works with cross-functional teams (e.g., Infrastructure, DevOps, Security Operations) to ensure smooth integration of Zero Trust technologies, such as identity and access management (IAM), multi-factor authentication (MFA), network segmentation, and endpoint security.
- Designs and develops a comprehensive Zero Trust architecture tailored to the organization's specific security needs and business objectives.
- Ensures access control policies are developed and implemented to ensure appropriate enforcement of a zero trust security model. Monitors compliance.

- Collaborates with relevant stakeholder to develop, update, and enforce network security policies and procedures.

5% (E) **Security Program Support**

- Contributes to the development and maintenance of information security policies and procedures.
- Participates in program, administrative, or operational reviews and audits of information security programs to ensure programs and operations are meeting established goals/objectives and regulatory guidelines.
- Performs or supports forensics requests including event history, e-discovery, etc.; provides analysis of findings.
- Develops and documents procedures to support new processes or process changes, as needed, to support implementation.
- Develops technical roadmaps and designs, enterprise architecture security standards, and strategies to best align technology solutions with business and organizational needs.

5% (E) **Other Duties**

- Fosters an environment of teamwork and collaboration, communicates position related information, and promotes the exchange of ideas through active listening and open discussion.
- 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 and information security.
- Invests in personal development through continuous education to gain and enhance position-related knowledge
- Ensures travel is approved and documentation and expense claims are processed in a timely manner
- Adheres to Authority policies and procedures regarding attendance, leave, and conduct.
- Other IT duties as needed to accomplish the Authority'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 ☒	Yes ☒ No ☐	Yes ☐ No ☒	Yes ☐ No ☒	Yes ☐ No ☒
Type:		Language:		

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

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.

Knowledge and Abilities

All knowledge and abilities of the Information Technology Specialist I classification; and

Knowledge of: Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

Desirable Qualifications

- Associate or bachelor's degree in an information technology related field of study.
- Five (5) years of experience in Information Security Operations.
- Possess of one or more of the following certifications (active):
  - Associate of $(ISC)^2$
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Auditor (CISA)
  - CompTIA Security+
  - CompTIA PenTest+
  - GIAC Information Security Fundamentals
  - AWS Certified Solutions Architect Associate
  - AWS Certified SysOps Administrator Associate
  - Microsoft Certified Azure Administrator
  - Microsoft Certified Azure Security Engineer
- Experience with Windows-based operating systems, configurations, Active Directory, and Group Policy.
- Experience managing Endpoint Detection & Response (EDR) solutions such as CrowdStrike and Microsoft Defender.
- Knowledge of cloud computing platforms such as Amazon Web Services or Microsoft Azure.
- Knowledge of penetration testing tools like Burp Suite, Nmap, Nessus, and Wireshark.
- Knowledge of Zero-Trust Networking and Center for Internet Security (CIS) Controls and Benchmarks.
- Knowledge and thorough understanding of NIST, SAM, and SIMM.
- Demonstrated ability to exercise good judgement in the performance of responsibilities, requiring minimal supervision.
- Demonstrate a talent and passion for information security, creativity, and resourcefulness in solving problems.
- Ability to think critically and independently analyze and resolve issues.
- Ability to meet business needs through innovative solutions and demonstrate a service oriented, customer relations-sensitive attitude.
- Ability to establish and maintain cooperative working relationships with all levels of staff and management; 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, technical diagrams, information security policies, etc.).
- Exhibit a talent and passion for information security.

- Willingness to work excess hours to achieve business results.
- Display enthusiasm for continuous learning.

Supervision Exercised Over Others

This position does not supervise others but may act in a lead capacity. The incumbent will have defined responsibility and authority for decision making related to projects or in an advisory function.

Public and Internal Contacts

The incumbent will have regular contact with various levels of staff at the Authority, consultants, vendors, contractors, 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

At the Information Technology Specialist II level, incumbents are responsible for independent work within business constraints. This level is responsible for the recommendations to executives, decisions for the projects, and outputs. As a subject matter expert; this level is responsible for actions that could have a serious detrimental effect on the operating efficiency of the undertaking or function. The consequence of error at the Specialist 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, and loss of business continuity. Consequences also include error in making decisions or giving advice that would have a serious detrimental effect on the operating efficiency of the undertaking or function.

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. Specific schedules will be set between the supervisor and the employee.
b. Telework: Part time telework is available for this position with a minimum of two in-office working days per week.
c. Travel: Occasional travel to Authority locations in California, may be required.
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: