STATE OF CALIFORNIA • DEPARTMENT OF TRANSPORTATION

POSITION DUTY STATEMENT

PM-0924 (REV 01/2022)

CLASSIFICATION TITLE	OFFICE/BRANCH/SECTION	
Information Technology Manager II		
WORKING TITLE	POSITION NUMBER	REVISION DATE
CalSTA Agency Cybersecurity Compliance Officer		1/3/2023

As a valued member of the Caltrans leadership team, you make it possible for the Department to provide a safe and reliable transportation network that serves all people and respects the environment.

GENERAL STATEMENT:

Under administrative direction of the CalSTA Agency Information Security Officer (AISO), the CalSTA Agency Cybersecurity Compliance Officer (Information Technology Manager II) has broad oversight responsibility for ensuring the Cybersecurity activities within the CalSTA Departments and Organizations are in compliance with the State of California Department of Technology (CDT) policies, the State's legislative and legal requirements as well as adherence to industry-specific regulations (such as the Payment Card Industry cybersecurity requirements).

The incumbent directs the complex compliance activities in close alignment with the CalSTA Department Chief Information Security Officers (CISOs) and the managers and supervisors throughout the Information Technology (IT) areas as well as the Business Program management.

CORE COMPETENCIES:

As an Information Technology Manager II, the incumbent is expected to become proficient in the following competencies as described below in order to successfully perform the essential functions of the job, while adhering to and promoting the Department's Mission, Vision, Values, Strategic Imperatives and Goals. Effective development of the identified Core Competencies fosters the advancement of the following Leadership Competencies: Change Commitment, Risk Appetite, Self-Development/Growth, Conflict Management, Relationship Building, Organizational Awareness, Communication, Strategic Perspective, and Results Driven.

TYPICAL DUTIES:

Percentage	Essential (E)/Marginal (M)[1]	Job Description
35%	E	Leadership: The incumbent provides the leadership for the development and continuous improvement of people, processes and technology to support CalSTA Cybersecurity Compliance activities and reporting at all CalSTA Departments and Divisions including Board of Pilot Commissioners (BOPC), California Highway Patrol (CHP), California Transportation Commission (CTC), Department of Transportation (Caltrans), Department of Motor Vehicles (DMV), High-Speed Rail Authority (HSR), Office of Traffic Safety (OTS), and New Motor Vehicle Board (NMVB). Provides the leadership for the development and improvement of cybersecurity compliance activities and reporting at these entities. Directs establishing and maintaining cybersecurity standards within each CalSTA Division and Department for the analysis, design, implementation, maintenance and operation of cybersecurity compliance. Represents the CalSTA Cybersecurity Compliance Agency-wide view in internal and external meetings. The compliance activities will help bridge the gap between the awareness of deficiencies and the resolution actions needed (through the timely delivery of information to the right leaders using reliable and trustworthy analysis biased on industry best practices, and expert guidance).

30%	E	Policy and Reporting: Coordinate Office of Information Security (OIS) compliance and reporting requirements with entity Chief Information Security Officers at CalSTA constituent entities. Provides performance measurement reporting for CalSTA and Division/Department Leadership with respect to Technology Recovery Plan Review and Testing Coordination (including applicable backup and restoration compliance activities to support enterprise data recovery). Guides constituent Divisions and Departments in the implementation and compliance with system security baseline configurations. Develops appropriate controls for system audit events and security information and event management (SIEM) retention of audit events. Guides the development of data/media retention and disposal policy and compliance reporting. Leads the Agency Divisions and Departments in the implementation and compliance reporting of IT asset inventory and ownership. Leads the cybersecurity third-party compliance requirements (for example the contract terms and conditions) for contractors and vendors doing business with CalSTA constituent organizations. Leads software development and coding cybersecurity compliance policy development and compliance measurements and reporting. Coordinate cybersecurity compliance workforce requirements and succession planning.
30%	E	Planning and Remediation: Be informed of cybersecurity compliance issues and assist in compliance gap remediation planning activities. Provide consistent and standardized planning process and approach to cybersecurity incident remediation preparedness efforts and reporting across CalSTA to the State Office of Information Security, the Agency Information Security Officer and the State Chief Information Security Officer. Develop, maintain and oversee cybersecurity compliance reporting process and policy requirements and facilitate the development of cybersecurity incident prevention compliance efforts.
5%	M	The incumbent conducts analysis across all CalSTA Divisions and Departments which requires attending meetings at a variety of levels across the organizations and with Leadership at all levels including Department Directorship and Agency Secretaries. Prepares and delivers executive summary presentations for internal and external audiences and performs data analytics and data visualization activities with a strong background and grounding in all aspects of Information Technology as well as Operational Technology. Empowers decision makers through distilling complex multi-variate problems into trade-off decisions for non-technical audiences.

[1]ESSENTIAL FUNCTIONS are the core duties of the position that cannot be reassigned.
MARGINAL FUNCTIONS are the minor tasks of the position that can be assigned to others.

SUPERVISION OR GUIDANCE EXERCISED OVER OTHERS

This position oversees cybersecurity compliance activities at all CalSTA constituent Divisions and Departments. The compliance activities are performed by a variety of Information Technology managers, supervisors, their staff, State contractors, and business program staff, managers, supervisors and contractors.

KNOWLEDGE, ABILITIES, AND ANALYTICAL REQUIREMENTS

Data analytics skills including the ability to use data visualization tools.

Familiarity with database systems and data integrity concepts, data encryption standards and data security concepts.

Understand technology recovery planning and system resilience as well as application programming interfaces to facilitate the technology implementation of a cybersecurity tool architecture that supports data insight generation through cybersecurity cross-tool (data) integration.

Understanding of, and familiarity with industry standard cybersecurity compliance requirements, especially the National Institute of Standards and Technology (NIST) Section 800-53. Understand the standards, guidelines and best practices for cybersecurity and their practical application from a variety of sources including industry, Federal and State government standards and statutory/legal requirements.

Understanding of email security, phishing/spam protections as well as cloud cybersecurity fundamentals and cloud cybersecurity best practices.

Understand and familiar with fundamental cybersecurity concepts such as Zero Trust, Identity Threat Detection and Response,

Endpoint Detection and Response, cryptography and edge protections and tools.

Understands cybersecurity audit and accountability procedures as well as the types of events that should be audited, non-repudiation of audit event log events, audit log monitoring and how audit events are to be preserved in a security information and event management (SIEM) system for further analysis.

Is familiar with system configuration cybersecurity baseline standards such as the United States Government Configuration Baseline (USGCB) and the Defense Information Systems Agency Security Technical Implementation Guide (STIG) for system hardening.

Understands foundational network principles and computer system communication protocols, network traffic anomalies, and encryption fundamentals.

Understands the foundational concepts for secure coding practices and software supply-chain protections.

RESPONSIBILITY FOR DECISIONS AND CONSEQUENCES OF ERROR

The incumbent must exercise good judgment, analyze problems, and take appropriate action. Poor decisions or recommendations could result in weaknesses in the CalSTA privacy and cybersecurity protections which increases the likelihood of a data breach, identity theft or a successful cybersecurity attack against a CalSTA constituent Department or Division.

PUBLIC AND INTERNAL CONTACTS

The incumbent interacts with IT executive leadership, staff of other State Agencies including State Control Agencies, staff from local governmental agencies and staff working in the private sector to coordinate and respond to inquiries related to cybersecurity and privacy policy, compliance and risk. In performing the responsibilities of this position, the incumbent may have contact with other departments, governmental agencies or private companies concerning cybersecurity, privacy, information technology, operational technology and business management best practices. Must develop and maintain strong working relationships with others.

PHYSICAL, MENTAL, AND EMOTIONAL REQUIREMENTS

The employee may be required to sit for prolonged periods of time using a keyboard, monitor, mouse, and telephone. Employee must value cultural diversity and other individual differences in the workforce; adjust rapidly to new situations warranting attention and resolution; be open to change and new information; adapt behavior and work methods in response to new information, changing conditions, or unexpected obstacles; consider and respond appropriately to the needs, feelings, and capabilities of others; be tactful and treat others with respect. In addition, the employee must have the ability to multi-task, adapt quickly to changing priorities, and perform completed staff work or tasks and projects with short notice.

WORK ENVIRONMENT

The incumbent may be required to work outside normal business hours, extended hours, weekends, and holidays and may be required to travel (primarily to locations within California).

The incumbent must carry a State-issued cell phone and respond to calls during and outside of normal business hours.

I have read, understand and can perform the duties listed above. (If you believe you may require reasonable accommodation, please discuss this with your hiring supervisor. If you are unsure whether you require reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Reasonable Accommodation Coordinator.)

EMPLOYEE (Print)	
EMPLOYEE (Signature)	DATE

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

SUPERVISOR (Print)	
SUPERVISOR (Signature)	DATE