STATE OF CALIFORNIA • DEPARTMENT OF TRANSPORTATION

POSITION DUTY STATEMENT

DOT PM-0924 (REV 01/2025)

CLASSIFICATION TITLE	OFFICE/BRANCH/SECTION	
C.E.A.	D20/IT/Security Services Division	
WORKING TITLE	POSITION NUMBER	REVISION DATE
Chief Information Security/Privacy Officer	900-170-7500-005	7/23/25

As a valued member of the Caltrans team, you make it possible to improve lives and communities through transportation.

GENERAL STATEMENT:

Under the general direction of the Deputy Secretary of Technology, Agency and Chief Information Officer,Caltrans, the incumbent has broad administrative participation in the formulation, operation and evaluation of the Department's Security Services Division on issues affecting information security, operational recovery and network technologies. The Chief Information Security/Privacy Officer develops and oversees the implementation of policies associated with cybersecurity risk management industry standards and State policy to identify and assess risk associated with the Department's information security assets.

CORE COMPETENCIES:

As a C.E.A., 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.

- **Change Leadership:** Develops new and innovative approaches needed to improve effectiveness and efficiency of work products. Encourages others to value change. Considers impact and recommends changes. (Employee Excellence - Collaboration)
- **Decision Making:** Makes critical and timely decisions. Takes charge. Supports appropriate risk. Makes challenging and appropriate decisions. (Employee Excellence - People First)
- **Initiative:** Ability to identify what needs to be done and doing it before being asked or required by the situation. Seeks out others involved in a situation to learn their perspectives. (Safety - Integrity)
- **Problem-solving and Decision-making :** Identifies problems and uses logical analysis to find information, understand causes, and evaluate and select or recommend best possible courses of action. (Climate Action - Integrity)
- **Relationship Building:** The ability to develop and maintain internal and external trust and professional relationships, which includes listening and understanding to build rapport. (Equity - People First)
- **Organizational Awareness:** Contributes to the organization by understanding and aligning actions with the organization's strategic plan, including the mission, vision, goals, core functions, and values. (Employee Excellence - Stewardship)
- **Influencing Others:** The ability to gain the support of others for ideas, proposals, projects and solutions. (Employee Excellence - Collaboration)
- **Vision and Strategic Thinking:** Communicates the "big picture". Models the department's Vision and Mission to others. Influences others to translate vision into action. Future oriented, and creates competitive and break through strategies and plans. (Prosperity - Innovation)
- **Commitment/Results Oriented:** Dedicated to public service and strives for excellence and customer satisfaction. Ensures results in their organization. (Employee Excellence - Innovation)

TYPICAL DUTIES:

Percentage	Essential (E)/Marginal (M)[1]	Job Description
25%	E	Strategic Leadership and Policy Development: Lead the development and execution of a department-wide information security strategy and policies aligned with Caltrans strategic plan, state laws, regulations, State policies and State strategies including Cal-Secure. Formulate and implement aligned information security policies and practices that address strategic initiatives, deficiencies found in cybersecurity assessments and audits. Continuously assess and revise these policies and practices to adapt to new cybersecurity threats and Information Technology/Operational Technology (IT/OT) advancements to protect the Caltrans enterprise information technology networks as well as the Caltrans OT networks containing field elements such as traffic signals, changeable message signs, roadside sensors, traffic and security cameras, Programmable Logic Controller (PLC) systems and Supervisory Control and Data Acquisition (SCADA) systems.

Americans with Disabilities Act (ADA) Notice: This document is available in alternative accessible formats. For more information, please contact the Forms Management Unit at (279) 234-2284, TTY 711, in writing at Forms Management Unit, 1120 N Street, MS-89, Sacramento, CA 95814, or by email at Forms.Management.Unit@dot.ca.gov.

25%	Compliance, Governance and Risk Management: Identify, evaluate, and mitigate cybersecurity and privacy risks. Ensure regular third-party security assessments and audits are conducted through the California Department of Technology (CDT) and California Military Department. Ensure compliance with the State of California Laws, Government Codes, the State Administrative Manual (SAM), Payment Card Industry (PCI) requirements and the State Information Management Manual (SIMM). Develop governance frameworks aligned to the statewide policies and Caltrans' Department policies to manage information security for enterprise IT systems and users, legacy systems such as mainframe systems and data, cloud-hosted services as well as the data exchange/connectivity interfaces between these systems (both on premises as well as off premises). Work with Caltrans Traffic Ops and Maintenance engineers to develop cybersecurity operational policy guidance for SCADA, PLC and OT systems and data.
20%	Incident Response and Recovery: Develop and manage the Department's cybersecurity incident response plans. Direct regular tabletop exercises to ensure organization cybersecurity incident response readiness. Ensure tabletop lessons learned and findings are addressed and remediated. Oversee efforts in cybersecurity incident investigation, digital forensics and system recovery. Ensure digital forensics capabilities are legally defensible preservation of data adhering to industry standard digital forensics best practices. Serve as the Department's "person most qualified" in legal depositions and testimony to describe and defend digital forensics preservation of evidence and digital forensic investigations and findings.
20%	Team Management, Contract Management and Stakeholder Engagement: Lead and mentor the management and staff of the Security Services Division within Caltrans Information Technology. Direct and oversee the resource allocation, performance evaluation, and professional development of the team. Direct reports include an IT Manager II and senior-level technical staff (Information Technology Specialist IIIs). Provide a work environment free from discrimination, harassment and retaliation by instructing managers and supervisors to monitor the implementation of the Caltrans Equal Employment Opportunity (EEO) programs and compliance of business activities with EEO guidelines and directives. Develop budget change proposals and gain support for additional budget and staff resource allocations to support the expansion of the cybersecurity program in response to additional, identified cybersecurity resource needs. Direct and oversee the budgeting process, contract management and approve expenditures for the Division.
5%	Reporting and Communication: Provide regular reports on the status and posture of information security and privacy within the department to executive management, the Caltrans Director's Office, and State oversight agencies including the CDT. Directs the activities to provide required compliance reports to the CDT in compliance with the State Administrative Manual and State Information Management Manual reporting requirements.
5%	Continuous Improvement: Stay abreast of the latest trends in cybersecurity and new technologies. Integrate innovative solutions and best practices into the department's cybersecurity strategies in support of the digitization of transportation in alignment with the California State Transportation Agency (CalSTA) priorities and the Caltrans strategic plan.

[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

The incumbent will directly supervise one IT Manager II and indirectly, the overall staffing of the Security Services Division.

KNOWLEDGE, ABILITIES, AND ANALYTICAL REQUIREMENTS

Knowledge of: principles, practices, and trends in public administration, including management, organization, planning, cost/ benefit analysis, budgeting, and project management and evaluation; employee supervision, workforce development and training, personnel management, modern computer forensic policies and safety and health policies; managerial skills and technical expertise related to Information Security, Risk Analysis, Business Continuity Planning and Operational Recovery Planning; physical security methods and techniques as applied to information and information systems; information systems change control process and procedures as related to information security; hardware and software involved in the design, operation and maintenance of an enterprise network; current equipment and techniques for voice and data communication in a network environment; State and federal laws and regulations concerning the proper acquisition, use and storage of intellectual property

Americans with Disabilities Act (ADA) Notice: This document is available in alternative accessible formats. For more information, please contact the Forms Management Unit at (279) 234-2284, TTY 711, in writing at Forms Management Unit, 1120 N Street, MS-89, Sacramento, CA 95814, or by email at Forms.Management.Unit@dot.ca.gov.

and data; federal and international laws pertaining to the information security.

Ability to: communicate ideas and information effectively both orally and in writing; provide clear and concise presentations to targeted audiences; act as “expert witness” on matters related to information security; as “subject matter expert” on behalf of the Department; effectively perform and direct multiple, high priority projects simultaneously; reason logically and creatively take appropriate actions; establish and maintain priorities; gain and maintain the confidence and cooperation of others.

RESPONSIBILITY FOR DECISIONS AND CONSEQUENCES OF ERROR

The incumbent has extensive decision making authority by initiating key actions and influencing key decisions. Policy decisions will directly impact departmental practice regarding the security and integrity of its information and information systems; and its ability to recover in the event of a disaster. If decisions and/or recommendations are not accurate or timely, the security and confidentiality of the Department’s information assets may become vulnerable and its ability to maintain its essential functions may be impaired.

PUBLIC AND INTERNAL CONTACTS

Incumbent will routinely interface with Executive Management staff, both in the District and in Headquarters, the Director’s office, as well as Information Technology staff and Budget Office staff. External contacts may include international, national, State and private sector information security contacts, Business, Transportation & Housing Agency, the Governor’s office and other Legislative Offices. The incumbent will represent the Department at various conferences and seminars. Will also have occasional contact with contractors/vendors and members of the public at large.

PHYSICAL, MENTAL, AND EMOTIONAL REQUIREMENTS

incumbent 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 incumbent must have the ability to multi-task, adapt quickly to changing priorities, and perform completed staff work or tasks and projects with short notice. Regular and consistent attendance is critical to the successful performance of this position due to the heavy workload and time-sensitive nature of the work. The incumbent routinely works with and is exposed to sensitive and confidential issues and/or materials and is expected to maintain confidentiality at all times.

WORK ENVIRONMENT

This position may be eligible for telework. The amount of telework is at the discretion of the Department and based on Caltrans’s current telework policy. While Caltrans supports telework, in-person attendance may be required based on operational needs. Employees are expected to be able to report to their worksite with minimal notification if an urgent need arises, as determined by the Department. The selected candidate may be required to travel to the headquartered location. All expenses to travel to the headquartered location will be the responsibility of the selected candidate.

Americans with Disabilities Act (ADA) Notice: This document is available in alternative accessible formats. For more information, please contact the Forms Management Unit at (279) 234-2284, TTY 711, in writing at Forms Management Unit, 1120 N Street, MS-89, Sacramento, CA 95814, or by email at Forms.Management.Unit@dot.ca.gov.

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.)

I agree that by providing my electronic signature for this form, I agree to conduct business transactions by electronic means and that my electronic signature is the legal binding equivalent to my handwritten signature. I hereby agree that my electronic signature represents my execution or authentication of this form, and my intent to be bound by it.

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

Americans with Disabilities Act (ADA) Notice: This document is available in alternative accessible formats. For more information, please contact the Forms Management Unit at (279) 234-2284, TTY 711, in writing at Forms Management Unit, 1120 N Street, MS-89, Sacramento, CA 95814, or by email at Forms.Management.Unit@dot.ca.gov.