State Treasurer's Office
POSITION DUTY STATEMENT
STO 1000 (Rev 11/2025)

DIVISION OR BCA					POSITION NUMBER (Agency-Unit-Class-Serial)	Position ID
Information Technology (IT)					820-760-7500-002	327
UNIT					CLASSIFICATION TITLE	
Cybersecurity					C.E.A. A	
TIME BASE / TENURE	CBID	WWG	COI	MCR	WORKING TITLE	
Full Time/Permanent	M01	E	Yes ☒ No ☐	1	Chief Information Security Officer (CISO)	
LOCATION					INCUMBENT	EFFECTIVE DATE
Sacramento						

STATE TREASURER'S OFFICE MISSION

The State Treasurer's Office (STO) provides banking services for state government with goals to minimize banking costs and maximize yield on investments. The Treasurer is responsible for the custody of all monies and securities belonging to or held in trust by the state; investment of temporarily idle state and local government monies; administration of the sale of state bonds, their redemption and interest payments; and payment of warrants drawn by the State Controller and other state agencies.

DIVISION OR BCA OVERVIEW

BRIEFLY DESCRIBE THE DIVISION/UNIT FUNCTIONS

The Information Technology Division (ITD) is the internal technology service organization that provides information processing support to the Divisions of the State Treasurer's Office and its associated Boards, Commissions, and Financing Authorities. The mission of the ITD is to assist the Divisions, Boards, Commissions, and Financing Authorities in achieving their program objectives through the efficient and effective delivery of quality information technology products and services.

This mission is accomplished through the combined efforts of several ITD teams: Cybersecurity, Technology Acquisition, Application Management, IT Service Desk, Collaboration Services, and Network and Systems Support. Working together, these IT teams offer a full range of services, including application development and modernization, data center and cloud services, information security, network engineering and support, infrastructure development, equipment and software procurement, desktop support, web presence, technology-related project management, and technical support for new and emerging technologies.

GENERAL STATEMENT

BRIEFLY (1 OR 2 sentences) DESCRIBE THE POSITION'S ORGANIZATIONAL SETTING AND MAJOR FUNCTIONS

Under the general direction of the Chief Information Officer (CIO), the Chief Information Security Officer (CISO) serves as a high level executive authority for cybersecurity policy, strategy, and enterprise security governance. The CISO provides high-level direction on cybersecurity risks and investments, advises executive leadership on statewide and departmental policy impacts, and ensures the confidentiality, integrity, and availability of STO's information assets. The incumbent has broad responsibility for shaping and implementing long-range cybersecurity strategies and ensuring compliance with state and federal mandates. The CISO leads the information security program and exercises significant policy-making authority across all cybersecurity functions.

% of time performing duties	Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first.
30%	**Executive Leadership, Policy Development, and Strategic Governance** Provides executive leadership in establishing and governing STO's enterprise cybersecurity vision, policies, standards, and long-range strategies. Exercises broad discretionary authority to define cybersecurity governance structures, develops and modernizes enterprise-wide security policies, and ensures alignment with statewide directives, federal and state law, industry frameworks, and national best practices. Advises the CIO and STO executive leadership on strategic cybersecurity risks, resource needs, investments, and the long-term operational and policy implications of emerging threats and evolving technologies. Leads enterprise security planning, establishes strategic priorities, and ensures cybersecurity governance is fully integrated into business operations, technology procurement, system design, and department-wide program planning. Monitors industry trends, evaluates emerging technologies, assesses innovative tools and frameworks for potential adoption. Formulates policy recommendations and proposes innovative, secure solutions that enhance the resilience, performance, and security of STO's information systems and technology services.
25%	**Enterprise Risk Management, Compliance Oversight, and Regulatory Assurance**

	Establishes and governs STO's enterprise cybersecurity risk management framework, ensuring continuous compliance with statewide security policies, statutory mandates, and recognized cybersecurity standards. Leads enterprise risk assessments, identifies and prioritizes cybersecurity risks across STO programs and business units, and sets policy-level mitigation requirements to strengthen STO's overall risk posture. Leads internal and external audits, Privacy Threshold Assessments and Privacy Impact Assessments, statewide security assessments, and compliance reviews, ensuring that corrective actions are implemented consistently, sustainably, and in alignment with enterprise policy. Ensures STO meets all applicable requirements of the State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), NIST Cybersecurity Framework, NIST Secure Software Development Framework, FIPS 199/200, AB 2135, and other binding federal and state regulations. Leads the development, implementation, and annual validation of Technology Recovery Plans, continuity strategies, and operational resiliency frameworks, ensuring that all STO programs, systems, and IT environments maintain compliance and readiness for disruptive events. Review and negotiate security-related clauses in contracts and agreements with vendors, state agencies, and other external entities to ensure alignment with the organization's security policies and compliance requirements.
25%	**Oversight of Cybersecurity Operations, Incident Response Governance, and Security Architecture Policy** Provides executive oversight and policy-level direction for the State Treasurer's Office (STO) cybersecurity operations, incident response readiness, and enterprise security architecture. Defines the enterprise security control environment, establishes architecture standards, and ensures that all IT systems, platforms, applications, cloud services, and third-party integrations adhere to STO's cybersecurity policy framework. Formulates enterprise policies for vulnerability management, penetration testing, threat intelligence integration, privileged access governance, and the secure configuration of security platforms such as SIEM, EDR, PAM, and statewide or departmental security technologies. Leads the development, governance, and execution of the enterprise Cyber Incident Response Plan (IRP). Provides executive leadership during major cybersecurity incidents, coordinates cross-departmental and statewide response activities, and ensures timely and accurate reporting to oversight entities including CDT Office of Information Security (OIS), Cal OES California Cybersecurity Integration Center (Cal-CSIC), CMD, CISA, and other regulatory partners. Leads the development of enterprise playbooks, security engineering standards, Zero Trust Architecture guardrails, and other policy-driven controls to ensure consistent implementation across all STO IT environments. Establishes policy expectations for cybersecurity training, workforce awareness initiatives, and enterprise-wide security culture. Chairs the Change Advisory Board (CAB) meetings ensuring minimal service disruption and mitigating risk to the organization. Provide leadership and oversight to security operations center.
15%	**Executive Program Management, Interagency Integration, Workforce Leadership, and Stakeholder Engagement** Oversees the enterprise cybersecurity program structure, resources, and workforce planning strategy to ensure STO maintains the organizational capability and expertise required to meet policy and program objectives. Establishes expectations for staff performance, training, succession planning, and operational resiliency, delegating operational activities to subordinates while maintaining accountability for overall program outcomes. Provides executive direction to cybersecurity personnel to ensure alignment with enterprise policy, program objectives, and the department's long-term cybersecurity strategy. Collaborates closely with STO executive leadership, IT division management, business program partners, procurement officials, and legal/compliance offices to integrate cybersecurity requirements into major initiatives, contracts, technology acquisitions, and departmental projects. Serves as STO's primary executive representative to statewide cybersecurity organizations, federal partners, other state agencies, and key external stakeholders to support coordinated policy development, information sharing, and alignment with statewide cybersecurity readiness strategies. Act as the single point of contact from ITD for all PRA requests, collaborate with other ITD sections, and ensure data disclosure complies with SAM & SIMM guidelines; review data for confidentiality, security risks, or exemptions to ensure lawful disclosure. Communicates transparently with

	executives and governance bodies, delivering risk briefings, policy impact analyses, program performance reports, and strategic recommendations that inform department-wide decision-making related to cybersecurity.
5%	Performs other related duties as required

SPECIAL REQUIREMENTS

N/A

To be reviewed and signed by the supervisor and employee:

EMPLOYEE'S STATEMENT:

- *I HAVE DISCUSSED THE DUTIES AND RESPONSIBILITIES OF THE POSITION WITH MY SUPERVISOR AND RECEIVED A COPY OF THIS DUTY STATEMENT.*

EMPLOYEE'S NAME (Print)	EMPLOYEE'S SIGNATURE	DATE

SUPERVISOR'S STATEMENT:

- *I CERTIFY THIS DUTY STATEMENT REFLECTS CURRENT AND AN ACCURATE DESCRIPTION OF THE ESSENTIAL FUNCTIONS OF THIS POSITION*
- *I HAVE DISCUSSED THE DUTIES AND RESPONSIBILITIES OF THE POSITION WITH THE EMPLOYEE AND PROVIDED THE EMPLOYEE A COPY OF THIS DUTY STATEMENT.*

SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE