CALIFORNIA STATE TREASURER'S OFFICE

POSITION DUTY STATEMENT

☒ PROPOSED

□ CURRENT

DIVISION OR BCA Information Technology (IT)	POSITION NUMBER (Agency-Unit-Class-Serial) 820-740-1405-001	Position ID 153
UNIT Cybersecurity	CLASSIFICATION TITLE Information Technology Manager I	

TIME BASE / TENURE Full Time/Permanent	CBID M01	WWG E	COI Yes ☒ No □	MCR 1	WORKING TITLE Chief Information Security Officer

LOCATION Sacramento	INCUMBENT	EFFECTIVE DATE

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.

COMMITMENT TO DIVERSITY, EQUITY, AND INCLUSION

The California State Treasurer's Office (STO) is committed to building and fostering a diverse workplace. We believe cultural diversity, backgrounds, experiences, perspectives, and unique identities should be honored, valued, and supported. We believe all staff should be empowered. The STO is proud to foster inclusion and representation at all levels of the Department.

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 general direction of the Chief Information Officer (CIO), incumbent holds complete management responsibility for Cybersecurity section in IT division.

The Cybersecurity section provides essential services to safeguard STO's digital assets and sensitive information. These services include threat detection and analysis, vulnerability assessments, security policy development and enforcement, incident response and recovery, employee training and awareness programs, security technology deployment and management, technology recovery planning, and continuous monitoring to identify and mitigate cybersecurity risks, ultimately ensuring the organization's resilience against cyber threats.

The Chief Information Security Officer is responsible for overseeing STO's cybersecurity strategy and ensuring the protection of sensitive data and information systems. Their role includes managing security policies, implementing safeguards, conducting risk assessments, responding to security incidents, and staying updated on emerging threats and security technologies to maintain a robust cybersecurity posture.

% 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%	**Leadership and Management** **Strategic Planning** • Develop and communicate the organization's cybersecurity strategy and vision.

	• Identify opportunities for technology innovation and improvements in cybersecurity. • Provide leadership and guidance on cybersecurity initiatives and best practices. • Ensure alignment of cybersecurity efforts with business goals and risk tolerance. • Collaborate with executive leadership to prioritize cybersecurity investments. **Team Management and Mentoring** • Provide leadership, mentorship, and performance evaluations. • Foster a collaborative and innovative team culture. • Allocate tasks and responsibilities effectively. • Reviews work products for completeness, accuracy, and fulfillment of assignment requirements. • Create staff succession plan and back up coverage plan to ensure operational resiliency. • Ensure professional development and training for team members. **Project Planning and Management** • Define project scopes, objectives, and deliverables for cybersecurity related projects. • Develop project plans, timelines, and resource allocation. • Monitor project progress, identify and mitigate risks. • Coordinate with stakeholders to ensure alignment with business goals. • Manage project budgets and resource allocation. Participate in preparing budget documents, including Project Approval Lifecycle (PAL) and Budget Change Proposals (BCP).
30%	Work independently as well as provide day-to-day supervision, technical oversight, and lead subordinate staff in the following service areas : **Risk Management and Compliance** • Identify, assess, and prioritize cybersecurity risks. • Proactively analyze information about cybersecurity intrusions and adversary adaptation and derive insights into which security measures could be most effective in limiting impact and harm. • Develop and implement risk mitigation strategies and controls. • Ensure compliance with industry regulations, data protection laws, and cybersecurity standards. • Lead regular internal security audits and assessments. • Facilitate external information security audits and collaborate to resolve security related assessment findings. • Lead staff in the development of STO's technology recovery plans, including development, maintenance, and annual drills. **Security Operations** • Oversee the day-to-day security operations, including monitoring, incident detection, and response. • Manage security tools and technologies, such as SIEM systems, intrusion detection systems, privileged access management system, etc. • Working collaboratively with other section managers, ensure that all information systems and IT assets are secure, whether on premise or located remotely or in cloud.

- Use current threat intelligence to hunt for threats in IT infrastructure, network, and applications based on identified exploitations and threats to the organization.
- Take steps to reduce the prevalence of exploitable vulnerabilities by providing authoritative instruction on prioritized mitigations.
- Ensure that vulnerabilities are fixed in a timely manner by driving remediation using all possible levers in collaboration with other ITD sections in STO.
- Develop, exercise, execute, and maintain the cyber incident response plan (IRP) to ensure effective coordination and reduction of the impact of cyber incidents.
- Develop and implement comprehensive training and awareness programs to promote information security and privacy best practices throughout the organization.
- Conduct internal penetration test on applications and infra to identify and document current attack vectors and current vulnerability exposures.
- Create actionable corrective action and remediation plans to mitigate or solve current exposures identified by penetration tests.

Security Architecture and Technology

- Define and maintain the organization's security architecture.
- Evaluate and select cybersecurity technologies and tools.
- Oversee the deployment and configuration of security solutions.
- Ensure the integration of security measures into IT infrastructure and applications.
- Identify gaps in the systems security design, recommend enhancements, and develop a roadmap to improve STO's security posture.
- Collaboratively drive implementation of specific actions, security controls, guardrails, and other mechanisms to align/comply with applicable sections of State Administrative Manual (SAM), the Statewide Information Management Manual (SIMM), National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), Federal Information Processing Standards (FIPS) 199 & 200 (Minimum Security Requirements), NIST Secure Software Development Framework (SSDF), AB 2135 (Information security), and other standards, frameworks, regulations (as applicable).
- Collaboratively develop guidance and technical criteria to help different teams in IT division to implement best practices (Zero Trust Architecture, Secure by Design, etc.), and to develop/implement secure and reliable systems and software.
- Create and engineer security information and event management (SIEM) rules, playbooks, and connections based on ITD's current and future tools and services.

Vendor and Third-Party Risk Management

- Assess and manage cybersecurity risks associated with third-party vendors and partners.
- Review and negotiate security clauses in contracts and service-level agreements.
- Conduct due diligence on vendor security practices.
- Ensure vendors comply with the organization's security requirements.

Incident Response and Recovery

- Develop and maintain an incident response plan and procedures.
- Lead incident response teams in investigating and mitigating security breaches, and provide post event resolution reports.
- Coordinate communication and reporting during and after security incidents.
- Implement recovery plans to restore normal operations.

Security Awareness and Training

	• Promote a culture of cybersecurity awareness throughout the organization. • Develop and deliver cybersecurity training programs for employees. • Keep staff informed about emerging threats and best practices.
15%	**Documentation and Reporting** • Create and maintain documentation for cybersecurity policies and procedures. • Prepare and provide security briefings and remediation plans by collecting and analyzing security related data from security infrastructure, various tools, and SaaS/PaaS/IaaS services implemented by ITD. • Report progress on projects and activities in meetings and provide regular written status reports.
5%	**Communication and Stakeholder Engagement** • Communicate project status and updates to executive leadership and stakeholders. • Collaborate with cross-functional teams (e.g., technology acquisition, network and systems support, workplace and collaboration services, application management, etc.) • Ensure effective communication within the team. • Establish and track tasks, priorities, dependencies, status and completion dates. • Report progress on projects and activities in meetings and provide regular written status reports. • Communicate effectively and develop and sustain cooperative working relationships with internal and external business partners. • Partner with other agencies and organizations such as California Department of Technology (CDT) Office of Information Security (OIS), California Governor's Office of Emergency Services (Cal OES) California Cybersecurity Integration Center (Cal-CSIC), California Military Department (CMD), Cybersecurity and Infrastructure Security Agency (CISA), etc. • Maintain all critical external reporting relationships and represent the STO when reporting security incidents and breaches to the appropriate authorities.
5%	**Research and Innovation** • Stay up-to-date with industry trends, emerging technologies, and best practices. • Research and evaluate new tools, frameworks, and technologies for potential adoption. • Propose innovative solutions to enhance application performance and security.
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