CALIFORNIA STATE TREASURER'S OFFICE

POSITION DUTY STATEMENT

☐ PROPOSED

☒ CURRENT

DIVISION OR BCA					POSITION NUMBER (Agency-Unit-Class-Serial)	Position ID
Information Technology (IT)					820-760-1402-002	154
UNIT					CLASSIFICATION TITLE	
Cybersecurity					Information Technology Specialist I	
TIME BASE / TENURE	CBID	WWG	COI	MCR	WORKING TITLE	
Full Time/Permanent	R01	E	Yes ☒ No ☐	1	Systems Security Specialist	
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 direction of the Chief Information Security Officer (CISO), an IT Manager I, incumbent is responsible for protecting STO's digital assets and sensitive information from cyber threats.

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 Systems Security Specialist is responsible for implementing, managing, and supporting enterprise security technologies and IT infrastructure components that protect the organization's systems, networks, and data. This role ensures alignment with organizational security policies, regulatory compliance frameworks, and industry best practices while maintaining availability and performance of core IT services. The incumbent will serve as a technical expert in enterprise security tools, infrastructure platforms, and endpoint protection systems.

% 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.
40%	Work independently as well as in collaboration with other cybersecurity staff in performing the following: **Security Tooling** • Administer, monitor, and optimize security tools including: o SIEM and incident response (Microsoft Sentinel) o Vulnerability management (Tenable) o Endpoint detection and response (Cortex XDR)

	o Privileged access management (Delinea) o Web Application Firewall (Imperva/Azure WAF) o Secure Managed File Transfer (MOVEit Transfer & Automation) • Analyze logs, alerts, and threat indicators across these platforms to proactively identify and respond to risks. **Endpoint Protection and Patch Management** • Manage and monitor endpoint protection strategies using appropriate tools (Cortex XDR.) • Implement and maintain patch management processes for: o Windows Servers using Azure Update Manager, WSUS, or SCCM. o Windows 10/11 laptops using Microsoft Intune and Windows Update for Business (WUfB). **Digital Identity, Certificates, and Remote Access** • Administer digital certificate lifecycle management (enrollment, renewal, revocation). • Maintain records and configurations for domain registrations. • Manage remote application solutions, ensuring secure connectivity for internal users and administrators. **Data Protection & Backup** • Support enterprise data protection, backup, and disaster recovery initiatives. • Validate backup integrity, enforce retention policies, and lead recovery testing. **Infrastructure Security and Shared Services** • Administer and secure core shared infrastructure services including: o Windows Active Directory (AD) and Group Policy o Domain Name System (DNS) o Dynamic Host Configuration Protocol (DHCP) o Network Time Protocol (NTP) o Secure Managed File Transfer (MFT) Ensure secure configurations and availability of these foundational services.
20%	**Virtualization and Systems Administration** • Support secure operation and configuration of VMware infrastructure. • Perform hardening and regular maintenance of Windows Server environments and storage systems. Manage server and storage environment to ensure alignment with security requirements.
15%	**Security Operations & Incident Response and Recovery** • Monitor cybersecurity alerts and advisories for common vulnerabilities and exposures, report significant security events and intrusions, and provide timely notice of imminent or hostile activities that may impact agency objectives, resources, or capabilities. • Proactively analyze information about cybersecurity intrusions and adversary adaptation, deriving insights into which security measures could be most effective in limiting impact and harm. • Utilize current threat intelligence to hunt for threats based on identified exploitations and threats to the organization. • Analyze logs, alerts, and threat indicators to identify anomalous activity and potential threats, coordinating with Network Security engineer and other IT staff. • Perform trend analysis and reporting, event correlation, and security reviews to identify security gaps and provide recommendations for inclusion in the risk mitigation strategy. • Create and engineer security information and event management (SIEM) rules, playbooks, and connections based on ITD's current and future tools and services. • 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.

	• 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. • Synthesize findings to develop robust and resilient vulnerability countermeasures to include in the architectural design. Collaborate in the development and maintenance of an incident response plan and procedures.
5%	**Collaboration** • 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. • Mentor and provide guidance to junior cybersecurity staff. Communicate effectively and develop and sustain cooperative working relationships with internal and external business partners.
10%	**Collaboration and Reporting** • 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 systems security projects and activities in meetings and provide regular written status reports.
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%	Perform 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