California Department of Tax and Fee Administration

DUTY STATEMENT

☐ CURRENT
☐ PROPOSED

SCHEDULE TO BE WORKED/WORKING HOURS		EFFECTIVE DATE	
CIVIL SERVICE CLASSIFICATION	**PRIMARY DOMAIN**	**WORKING TITLE**	
Information Technology Specialist I	System Engineering	Security Engineer	
DIVISION/OFFICE/UNIT		**SPECIFIC LOCATION ASSIGNED TO**	
TSD/EIB/Infrastructure Security Unit		Sacramento, CA - Headquarters	
SEERA DESIGNATION	**BARGAINING UNIT**	**WORK WEEK GROUP**	**CERTIFICATES REQUIRED**
Rank and File	01	E	None
FINGERPRINTS/ BACKGROUND CHECK REQUIRED	**BILINGUAL POSITION**	**SUPERVISION EXERCISED**	
☒ Yes ☐ No	☐ Yes ☒ No	None	
INCUMBENT		**POSITION NUMBER** *(Agency-Unit-Class-Serial)*	
		291 - 381 - 1402 - 151	

The mission of the California Department of Tax and Fee Administration is to make life better for Californians by fairly and efficiently collecting the revenue that supports our essential public services.

POSITION'S ORGANIZATIONAL SETTING AND MAJOR FUNCTIONS

Under the direction of the Information Technology Manager I (ITM I), the Information Technology Specialist I (ITS I) serves as an advanced member of the Infrastructure Security Unit. The ITS I is primarily responsible for the administration, monitoring, and analysis of the California Department of Tax and Fee Administration's (CDTFA) complex network infrastructure and security systems and acts as the high-level technical expert for a variety of enterprise network security system and infrastructure components. The ITS I is responsible for network security processes, software and hardware configurations, ensuring integrity and effectiveness of the enterprise network, and the security monitoring and protection of systems. The ITS I is tasked with ensuring that the enterprise network and its security systems comply with State and Federal regulations and industry accepted best practices.

The ITS I maintains a working level knowledge of the threat landscape, cloud security, network security, endpoint security, data security and regulatory compliance. Other responsibilities for this position include security incident response and communications, conducting internal audits and acting as a liaison for external security audits, drafting IT security procedures, reviewing security policies, reviewing and/or researching security design, technologies, trends and making recommendations for changes and upgrades to the network security and infrastructure environment.

Candidate must be able to perform the following essential job functions with or without reasonable accommodation.

PERCENTAGE OF TIME SPENT	DUTIES
	ESSENTIAL JOB FUNCTIONS
40%	Manage the hardware and software configuration of network security infrastructure systems, including Security Information and Event Management (SIEM), Intrusion Detection System/Intrusion Prevention System (IDS/IPS), firewalls, traffic analyzers, vulnerability scanners, network access control systems, web filtering solutions, and database activity monitoring and prevention systems. Continuously monitor network security events for anomalies, ensuring timely response and comprehensive reporting of findings. Conduct thorough identification and remediation of vulnerabilities through internal security audits, penetrations testing, vulnerability scanning and progress reporting. Detect, triage and investigate security incidents, active attacks, operational issues and performing detailed root cause analysis through Endpoint Detection and Response (EDR), SIEM, and other cyber defense applications. Regularly assess and analyze the network's security posture, providing actionable recommendations to leadership to enhance the organizational security framework in alignment with industry best practices and compliance regulations, including NIST SP 800-53, IRS Publication 1075, CISA Guidelines, OWASP Frameworks, and SAM/SIMM.
25%	Provide hands-on support for architecture, installation, configuration, deployment and patching of Enterprise Endpoint Protection hardware/software on-premises as well as cloud. Maintains endpoint protection strategies, principles, standards, and procedures that govern system and software maintenance and operations. Implement, support, and monitor identity protection to Active Directory, Entra ID and Security Center signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at the department. Configure and maintain anti-malware policies and manage Advanced Threat Protection systems to all CDTFA endpoints. Monitor and implement capabilities available in the Security Compliance Center for real-time detection/reporting, and automated incident response systems.

	Monitor and implement capabilities available in the Security Compliance Center for real-time detection/reporting, and automated incident response systems. Maintain Cloud Access Security Broker (CASB) for its various deployment modes and configure to provide required alerting and reporting.
20%	Conduct comprehensive reviews of network security and system design, including the evaluation of new systems and modifications to existing systems. Conduct and/or oversee the implementation, upgrade, patching, and decommissioning of security systems. Ensure continuous system availability by maintaining monitoring and reporting processes. Develop and refine security alerts to identify and notify personnel of potential security incidents requiring investigation. Continuously fine-tune alert configurations to enhance detection accuracy and regularly review and adjust alert parameters to ensure they effectively capture threats.
10%	Develop and maintain a comprehensive range of technical documentation including authoring and editing procedures, preparing annual and technical reports, and creating other supporting documents to effectively communicate complex technical information. Collaborate with the Information Security Office and Security Operation Center to establish and uphold security standards and processes that ensure compliance with NIST, IRS Publication 1075, FedRAMP and SAM/SIMM. Coordinate responses to data collection requests, status updates, and statistical reporting as necessary. Provide support for IT security assessments and audits.
	MARGINAL JOB FUNCTIONS
5%	Research and monitor the threat landscape, attack surfaces and stays current with the threat intelligence from OSINT, industry security alerts and notifications, threat intelligence feeds, vendor reports, and governmental advisories related to cybersecurity. Perform other related duties as required.

WORK ENVIRONMENT OR PHYSICAL ABILITIES REQUIRED FOR THE JOB (if applicable):

Work Environment:

- May work in a high-rise building.

Physical Abilities:

- Transport servers, PCs, printers, etc., that range in weight up to 50 pounds.
- Ascend/descend stairs, ladders, and function in confined workspaces.
- Move, bend, or reach while in the process of installing or relocating personal computers or other data communication equipment.

Additional Requirements/Expectations:

- Work long or irregular hours as needed.

I have read this duty statement and fully understand that I must perform the Essential Job Functions of my position with or without reasonable accommodation.

PRINT EMPLOYEE NAME	EMPLOYEE'S SIGNATURE	DATE

I certify that the above accurately represents the duties of the position and that I have reviewed these duties with the above-named employee.

PRINT SUPERVISOR NAME	SUPERVISOR'S SIGNATURE	DATE

HRB Approval Date: 04/14/2026	**C&P Analyst Initials: LLM**