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	Information Security	Security Operations Center (SOC) Analyst	
DIVISION/OFFICE/UNIT		**SPECIFIC LOCATION ASSIGNED TO**	
TSD/Security Operations Center		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	No	
INCUMBENT		**POSITION NUMBER** *(Agency-Unit-Class-Serial)*	
		291 - 381 - 1402 - 121	

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 Deputy Chief Information Security Officer/Privacy Officer, Information Technology (IT) Manager I, the Information Technology Specialist I (ITS I) is a member of the Security Operations Center (SOC) and the California Department of Tax Fee & Administration's (CDTFA) Cyber Incident Response Team. The ITS I demonstrates expertise in Security Operations and is a high-level technical security specialist. The ITS I will perform security operations duties on identification of information assets, security detections, security analysis and response activities to advance critical enterprise protection and to provide cyber defense of CDTFA information assets, taxpayer and employee information.

The ITS I creates and operates processes and tooling to establish and maintain comprehensive asset and network monitoring and defense against security threats across the enterprise's network infrastructure and user base. The ITS I works with enterprise-wide staff to prepare, detect and respond to attacks in a timely manner. The ITS I develops and maintains a working level knowledge of relevant IT infrastructure and technologies under the protection of the SOC, of applicable State/Federal and industry regulations and industry accepted best practices according to information security, policies and procedures, threat management and vulnerability, products, practices and processes. The ITS I also maintains a working level knowledge of the threat landscape, risk management processes, operating systems, cloud security, identity and access management, network architecture and protocols.

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

PERCENTAGE OF TIME SPENT	DUTIES
	ESSENTIAL JOB FUNCTIONS
50%	Performs timely day-to-day security tasks monitoring, analyzing and taking action on security alerts, notifications and findings from threat intelligence sources to protect and defend CDTFA's information assets, systems and infrastructure, on premises/cloud from threats using CDTFA's security tools. Documents all security actions taken and coordinates with enterprise-wide staff to determine validity of security alerts and escalates incidents that may cause continued and/or imminent impact to the environment. Ensures security products and tools mitigate or reduce identified risks to an acceptable level. Create, correlate, orchestrate and/or automate security alerts including Endpoint Protection Platform/Endpoint Detection & Response, Security Information & Event Monitoring system, Network Traffic Analysis & User Entity Behavioral Analytics, Identity sources, Phishing indicators, Application anomalies, Data Exfiltration and other cyber defense tools. Creates SOC standard operating procedures and guidelines. Performs security operations reviews, identify security gaps and provide recommendations to leadership to increase the organizational security posture according to industry accepted best practices and compliance regulations such as NIST publications, Publication 1075, CISA guidelines, CIS Controls, MS-ISAC, Cloud Security Alliance, OWASP and SAM/SIMM.
20%	Initiate incident response activities to identify, contain and remediate threats utilizing all available tools, logs and resources. Identify Tactics, Techniques, and Procedures (TTPs) of intrusion sets of malicious and/or anomalous activity on CDTFA assets. Initiate forensics response including triaging, live forensics, image acquisitions, timelines and root cause analysis on CDTFA information assets as needed.

15%	Monitors the threat landscape, attack surface and stays abreast of threat intelligence from sources such as OSINT, industry security alerts & notifications, threat intelligence feeds and as pertinent security events are discovered. Contextualizes threat intelligence security reports pertaining to vulnerability and exploit prioritization ratings in relation to CDTFA information assets and disseminates security reports to internal or external teams as needed.
10%	Configures and administers ISO security tools to protect and defend CDTFA's information assets, systems and infrastructure. Creates scripts or programs to aid in security detections and incident investigations. Creates real time security dashboards, reports, metrics and trend analysis. Provides support and coverage for other ISO team members as needed.
	MARGINAL JOB FUNCTIONS
5%	Perform other job-related duties as required.

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

Work Environment:

- Position may be located in a high-rise building
- Standard office environment (for example, artificial lighting, controlled temperature, etc)
- Requires being in a stationary position, consistent with office work, for extended periods of time
- Daily use of a personal computer, office equipment, and/or telephone

Physical Abilities:

-

Additional Requirements/Expectations:

- Work long, irregular or after hours as required

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: 09/10/2026	**C&P Analyst Initials: LLM**