DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 045 (REV. 03/2024)

Type of Duty Statement:	Current & Proposed	**Revision Date:**	01/14/2025

1. Position Information

A. Employee Name:

B. Position Number:	**C. CBID:**	**D. WWG:**	**E. Effective Date:**
817-415-1405-001	M01	E	

F. Classification Title:	**G. Working Title:**
Information Technology Manager I	Security Operations Center Manager

H. Division:	**I. Branch/Section/Unit:**
Technology Services	Enterprise Architecture & Security Branch / Security Operations Center

2. POSITION REQUIREMENTS

Special Requirement: *Check All that Apply*

- ☐ Bilingual Fluency (Non-English Language) - Specify Below
- ☑ Background Check Requirements
- ☐ Other - Specify Below

A. Special Requirements Description, as applicable:

N/A

B. Conflict of Interest Required (Gov. Code 87300, et seq.)? ☑ **Yes** ☐ **No**

This position is designated under the Conflict-of-Interest Code. This position is responsible for making or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete Form 700 within 30 days of appointment. Failure to comply with the Conflict-of-Interest Code requirements may void the appointment.

3. SUPERVISION

A. Supervision Received:

The incumbent reports directly to the Information Technology Manager II in the Enterprise Architecture & Security Branch.

B. Supervision Exercised:

The incumbent manages Information Technology (IT) staff in the Security Operations Center Section.

4. DUTIES AND RESPONSIBILITIES OF THE POSITION

CONDUCT, ATTENDANCE AND PERFORMANCE EXPECTATIONS

This position requires the incumbent conduct oneself in accordance with the Department of Child Support Services leadership practices and principles, maintain consistent and regular attendance; communicate effectively and professionally (both orally and in writing) in dealing with the public and/or other employees; develop and maintain knowledge and skills related to specific tasks, methodologies, materials, tools, and equipment; complete assignments in a timely and efficient manner; and adhere to all departmental policies and procedures.

GENERAL STATEMENT

This is the managerial level. Under the general direction of the Chief Information Security Officer (CISO), Information Technology Manager II (ITM II), the Information Technology Manager I (ITM I) have full supervisory and oversight responsibility for the Security Operations Center (SOC) Section, in the Enterprise Architecture & Security Branch, within Technology Services Division (TSD). The ITM I provides guidance and leads security response and forensics and oversees threat monitoring and threat hunting activities to ensure data and systems of the Department of Child Support Services (DCSS) and Local County Offices (LCSAs) stay protected. (DCSS and LCSAs are collectively referred to as 'DCSS' in this document).

A. Percentage of Time Performing Duties	**B. An itemized listing of the specific job duties and the percentage of time spent on each separate and distinct task, with essential and marginal functions identified. Percentages must be listed in descending order and must equal 100%. (No duties less than 5%.).**
	ESSENTIAL FUNCTIONS
IT Domain: *Check All That Apply*	**FOR INFORMATION TECHNOLOGY (IT) CLASSIFICATIONS ONLY** ☐ Business Technology Mgmt. ☐ Software Engineering ☐ IT Project Mgmt. ☑ System Engineering ☑ Information Security ☑ Client Services
35 %	SOC Management and Leadership: Responsible for the overall leadership and management of the SOC team and its operations. Ensures the effectiveness and efficiency of the SOC operations to minimize the impact of security incidents in DCSS and to maintain a high level of security posture. Ensures continuous 24x7 monitoring of DCSS. Develops or update policies, processes, procedures, and guidelines to ensure continuous 24x7 monitoring of DCSS, and compliance with DCSS and oversight agencies, such as, California Department of Technology (CDT) and IRS, regulations and requirements. Manages SOC team, including hiring and training team members. Conducts regular collaboration and communication sessions with CISO, Principal CyberSecurity Architect, Information Security Office, and Risk & Privacy Office, to discuss security strategies, security threats, security incident, key performance indicators and metrics, and executive reporting/dashboard. Communicates on the key SOC metrics and updates regularly to CISO, Principal CyberSecurity Architect, and DCSS Executives. Ensures that DCSS is in compliance with all applicable laws and rules regulating information security, confidentiality, and privacy by ensuring compliance with the Information Practices Act, the Public Records Act, and the disclosure provisions in the Revenue and Taxation Code and applicable federal Internal Revenue Service Disclosure requirements to limit departmental risk exposure.

30 %	Threat Monitoring, Detection, and Response Oversight: Analyzes as well as oversees team members conduct appropriate, thorough, and accurate analysis of security logs and alerts. Leads development and implementation of security controls and best practices to manage SOC activities. Manages fine tuning of security monitoring tools to reduce false positives and improve detection rates. Administers development and maintenance of incident response plans and playbooks. Acts as Incident Commander and lead incident response activities, including but not limited to, triage, investigation, containment, eradication, and recovery. Apprises CISO, Principal CyberSecurity Architect, IT Leadership team, and DCSS Executives on the incident situation and progress consistently following established DCSS communication plan. Consults and partners with Principal CyberSecurity Architect to procure and implement penetration testing technologies, develop testing processes and procedures, and lead testing exercises. Responds to written and verbal inquiries from the Health and Human Services Agency, DCSS Executives, CISO, Principal CyberSecurity Architect, and external parties on general SOC related or specific security incident related inquiries to ensure cooperation and collaboration across the enterprise.
20 %	Team Development and Management: Guides team and provides direction to team to maintain current knowledge of oversight agencies and DCSS policies and processes related to SOC. Develops training program to ensure SOC team members stay up to date on changing threat landscape and have relevant training to protect DCSS. Develops, updates, and maintains security incident response plans and conduct simulation and tabletop exercises to prepare DCSS to effectively respond to security incidents. Identifies appropriate metrics and data and leads team to create reports demonstrating the current security landscape, threat surface, and other SOC related information relevant to DCSS. Conducts performance reviews, write probation reports, assign staff work tasks, and address staff concerns. Fosters a culture of collaboration, continuous learning, and inquisitiveness to be constantly on the lookout for anomalies to prevent security breaches and incidents. Plans, organizes, and directs the staff involved in the development of necessary policies and procedures to safeguard DCSS data and systems. Monitors ongoing changes that can affect information security by managing staff workload that promote implementation enhancements to complex DCSS security policy and compliance areas to ensure improved services to DCSS customers.

10 %	Technology and Tools Management: Oversees the management and operations of various security tools and technologies, such as for, endpoint protection, network security, endpoint detection and response, security information & event management, intrusion detection, intrusion prevention, etc. Collaborates with manager, Principal CyberSecurity Architect, Information Security Office, Risk & Privacy Office to evaluate, select, and implement tools and technologies to enhance SOC capabilities. Acts as the expert on SOC related issues to ensure the SOC program is aligned with enterprise information security standards and federal regulations. Assesses security controls and documents the gaps and protection needs for DCSS systems, networks, and applications. Researches and presents emerging SOC related trends, tactics, vendors, and solutions to CISO and Principal CyberSecurity Architect and recommend proper course of action to improve DCSS security posture. Leverages available tools and technologies to administer security controls and operations to protect DCSS from security threats and incidents.
0 %	N/A

MARGINAL FUNCTIONS	
5 %	Provides overall support to the Department Executive management Leadership team, Chief Information Officer, Branch IT Manager II, and staff as the expert in Security Operations related topics. Represent the Enterprise Architecture & Security Branch on special teams, projects, and other duties as assigned. Perform special assignments, attend meetings, and serve as back-up for peers and the ITM II. Invest in personal
100 %	**TOTAL**

5. WORKING ENVIRONMENT AND PHYSICAL REQUIREMENTS

☐ **Office Centered**

Incumbent's workspace will be a two-story, office building environment with standard modular cubicle or office spaces, temperature control and artificial lighting. Requires sitting for long periods of time while using a personal computer for email communication, reviewing documents, and attending meetings. Incumbent must be able to sit for extended periods of time attending meetings or sit and/or stand while working. Incumbent may perform repetitive hand motions such as typing, push, pull, reach, or bend (neck and waist). The work environment is fast-paced and can be demanding. May require periodic work during non-standard hours and during weekends to meet workload needs. Travel may be required for meetings or to attend professional training and/or events.

☑ **Remote Centered**

Incumbent's workspace will be divided between an office-centered, two-story, professional office building environment and a remote-centered work location in accordance with an approved telework agreement. Dedicated remote-centered workspaces must comply with all departmental and state safety and security policies. Requires sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings remotely. The office-centered workspace consists of an office building environment with standard modular cubicle or hoteling office space, and artificial lighting. Requires sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings remotely or in designated areas. The work environment is fast-paced and can be demanding. May require periodic work during nonstandard hours and during weekends to meet workload needs. Travel may be required to attend professional training and/or events. Remote centered teleworkers must forgo telework when their physical presence is required in the office on a regularly scheduled telework day.

6. OTHER RESPONSIBILITIES

A. Independence of Action and Consequences:

Child Support Enforcement has critical timelines and political and financial ramifications. Poor participation, judgment, and decisions can adversely affect the success of the Child Support Program. Failure to identify risks and issues in a timely manner could result in slippages in schedule and increased costs. Poor communication and coordination can adversely affect the Child Support Program and the children of California. Incumbent is responsible for independent work within business constraints; recommendations to executives; decisions for projects and outputs; and program, project, and staff decisions and actions. Consequences may have statewide and enterprise-wide impacts, including lost funding, project failure, failed business strategy, poor customer service and performance, risk exposure, loss of business continuity, missed business opportunities, and budget implications.

B. Personal Contacts:

The incumbent has contact with departmental managers; supervisors; DCSS, state and LCSAs staff; governmental agencies; contractors; interface partners; and vendors.

C. Administrative Responsibilities (Supervisory/Managerial Class Only):

The incumbent performs the full range of supervisory and management duties, including, but not limited to: interpret and adhere to policies, rules, laws, regulations, and bargaining unit contracts; provide direction and guidance regarding work assignments and daily work activities to ensure timely completion of assignments; review work and evaluate performance of staff by providing regular feedback and completing timely probationary reports and annual performance appraisals summaries; monitor employee performance and, if necessary, utilize performance management principles and procedures; complete personnel documentation and utilize the competitive hiring process; and approve or deny administrative requests including leave, overtime, travel, and training.

7. Acknowledgements

A. Employee's Acknowledgement: I have read and understand the duties listed above and I certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others. I have received a copy of the duty statement.

I can perform these duties with or without reasonable accommodation: ☐ **Yes** ☐ **No**

If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will notify the Reasonable Accommodation Coordinator in the Equal Employment Opportunity and Diversity Office.

Duties of this position are subject to change and may be revised as needed or required.

Employee's Name (Print):	
Employee's Signature:	
Date:	

B. Supervisor's Acknowledgment: I certify this duty statement represents current and an accurate description of the essential functions of this position. I have discussed the duties of this position with and provided the above-named employee a copy of this duty statement.

Supervisor's Name (Print):	
Supervisor's Signature:	
Date:	