DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 046 (REV. 03/2024)

Type of Duty Statement:	Current & Proposed	**Revision Date:**	08/20/2026

1. Position Information

A. Employee Name:

B. Position Number:	**C. CBID:**	**D. WWG:**	**E. Effective Date:**
817-415-1414-002	R01	E	

F. Classification Title:	**G. Working Title:**
Information Technology Specialist II	Information Security Architect

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 I in the Security Operations Center.

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

Under the general direction of the Information Technology Manager I (ITM I), the Information Technology Specialist II (ITS II) has responsibility for ensuring the compliance and security of information technology information assets for the Department of Child Support Services (DCSS), within the Technology Services Division (TSD), Enterprise Architecture & Security Branch, in the Security Operations Center (SOC).

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
30 %	Lead the monitoring, reporting, and management of information security threats and incidents. Oversee information security investigations and track information security incidents to resolution. Develop and implement technical controls to safeguard DCSS' sensitive information from unauthorized use and access. Continuously lead the monitoring of security tools and systems, such as Security Information and Event Management (SIEM), to detect potential security incidents or anomalies, and prioritize responding to them based on severity and potential impact. Provide reports of incidents, findings from system assessments, and technical security documents to unit staff and management. Lead prompt and effective response to security incidents, following established response processes and procedures to contain, mitigate, and remediate incidents. Lead the proactive search, assessment, and remediation of advanced threats and vulnerabilities in systems, networks, and applications. Lead the analysis of logs from various sources and proactively optimize security tools to get accurate security alerts and insights. Ensure the performance of security checks to validate IT system compliance using endpoint protection and vulnerability management scanning and logging tools. Analyze security vulnerabilities, risks and exposures and communicate findings to relevant stakeholders to document security compliance deficiencies and actionable plans forward for remediation. Participate and communicate as a lead in the CyberSecurity Incident Response Team to a variety of stakeholders and executive staff members.

30 %	Create Information Security Architecture and verify models that communicate solutions securely and effectively to business users to ensure system changes meet the business user needs, as well as meet mandatory security standards and protocols. Translate ISA models into various formats to effectively communicate with diverse stakeholder groups. Lead unit staff in utilizing information security knowledge to make appropriate recommendations to the security controls framework. Prepares and provides security reports by collecting and analyzing security incidents data. Facilitate coordination and response to all security incidents and provide post event resolution summary to management. Identify gaps in the system's security design and recommend enhancements. Coordinate with DCSS and Local Child Support Agency (LCSAs) users to identify issues of considerable business consequence or importance and collaborate to ensure a thorough understanding of new or change in business objectives. Develop implementation plans for key aspects of ISA based on IT strategies to meet business requirements and support the efficient delivery of the programs, operations, and services.
20 %	Plan, configure, and manage security architecture and configuration of infrastructure, tools, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) services. Create and engineer SIEM rules, playbooks, and connections based on the enterprises current and future tool sets. Use current threat intelligence to hunt for threats in the enterprise's infrastructure, applications and identity platforms based on modern identified exploitations and threats to the organization. Develop test and deploy Endpoint Detection and Response (EDR), Network Detection and Response (NDR) and Extended Detection and Response (XDR) policies throughout the enterprise. Manage identity platform protections throughout the enterprise's identity stack. Review, configure and collaborate on networking device security configurations and rule sets to ensure secure and complaint configuration of devices. Conduct internal penetrations tests on applications and infrastructure to identify and document current attack vectors for the enterprise's current vulnerability exposures. Create actionable corrective action and remediation plans to mitigate or solve current exposures identified by penetration tests.

15 %	Serve as lead analyst and provide guidance to staff in the research, assessment, evaluation, and documentation of security changes to manage the DCSS Information Security policies, procedures, and standards. Ensure ISO policies, procedures and standards are compliant with state and federal requirements, industry standards and information security best practices. Review security-related documents and procedures for proposed changes to ensure Child Support Program data and functions and IT services are protected. Lead meetings, work groups, conferences, hearings, or presentations involving technical problems with business users and vendors to identify business challenges and provide solutions in alignment with the department's vision and strategic plans. Design and develop ISA artifacts, frameworks, and best practices to support DCSS systems. Guide the team, assign tasks within the work assignment, train, and mentor team members, and provide direction in alignment with the goals of the organization to ensure successful execution of the ISA in support of new DCSS initiatives.
0 %	N/A

MARGINAL FUNCTIONS	
5 %	Assist Chief Information Officer and TSD Managers & Supervisors in responding to initiatives. Represent Enterprise Architecture & Security Branch and TSD on special teams, projects, and in other duties as assigned. Perform special assignments, attend meetings, and serve as backup for Information Security staff.
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 participant, 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 individual decisions and actions. As subject matter expert, this level is responsible for actions that could have a serious detrimental effect on the operating efficiency of the undertaking or function. Consequence of error may result in loss of data, user dissatisfaction and impact to the organization, project or work unit and related support units. Consequences include operational downtime, loss of business continuity, poor customer service, and poor performance.

B. Personal Contacts:
The incumbent has contact with: DCSS executives, managers, supervisors, and staff; State and LCSAs staff; government agencies; contractors; interface partners; and vendors.

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:	