DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 046 (REV. 09/2026)

Type of Duty Statement:	Current & Proposed	**Revision Date:**	11/09/2026

1. Position Information

A. Employee Name:

B. Position Number:	**C. CBID:**	**D. WWG:**	**E. Effective Date:**
817-415-1402-002	R01	E	

F. Classification Title:	**G. Working Title:**
Information Technology Specialist I	CyberSecurity Defense Analyst

H. Division:	**I. Branch/Section/Unit:**
Technology Services	Information Security Office/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 direction of the Information Technology Manager I, the Information Technology Specialist I performs security monitoring, incident response, vulnerability and compliance analysis, and security tool administration to protect Department of Child Support Services (DCSS) information assets. The incumbent supports the Security Operations Center (SOC), in the Information Security Office, within Technology Services Division (TSD), and coordinates with technical teams to investigate threats, resolve security findings, and maintain effective security controls.

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
20 %	Security Monitoring and Incident Response: Monitor and analyze security alerts, incident reports, and suspicious activity received through the security operations mailbox, ServiceNow Security Incident Response, and monitoring platforms. Investigate malware, phishing, business email compromise, anomalous user activity, and endpoint, identity, network, cloud, and email security events to assess potential impacts. Conduct technical investigations and assigned forensic analysis in response to security events and authorized requests. Coordinate containment, remediation, and recovery activities with technical teams; preserve evidence; document response actions; and track incidents through resolution. Prepare summaries and supporting information for management review and authorized Cal-CSIRS reporting, and escalate significant or complex incidents to the team lead and SOC Manager. Respond to security service requests and recommend secure solutions for DCSS and Local Child Support Agency (LCSA) customers. Assist in reviewing and updating the Incident Response Plan, playbooks, and SOC procedures. Participate in tabletop exercises and playbook testing, and incorporate approved improvements and lessons learned into operational documentation.

20 %	Security Platform Administration and Automation Configure, maintain, and improve security monitoring and response platforms, including Security Information and Event Management, Security Orchestration, Automation and Response, and endpoint security tools. Develop, test, document, and maintain detection rules, response playbooks, integrations, and automated workflows to improve alert accuracy and response efficiency. Analyze tool performance, investigate logging and integration failures, and recommend corrective actions. Configure and validate Microsoft Defender for Endpoint and In-tune security settings in coordination with the endpoint administration team. Test proposed changes, assess operational impacts, and implement approved configurations through established change management procedures. Provide technical troubleshooting and backup support for SOC security platforms.
20 %	Vulnerability Analysis and Compliance Monitoring Review vulnerability scan results, security configuration assessments, and security advisories to identify affected systems, applications, and compliance deficiencies. Validate IT system compliance with approved security baselines and applicable departmental, state, and federal requirements using endpoint protection, vulnerability scanning, and logging tools. Compare scan coverage against the Configuration Management Database (asset inventory) to identify missing or not scanned assets. Analyze vulnerabilities, misconfiguration, and compliance findings; communicate results to responsible technical teams; and recommend corrective actions based on risk and departmental requirements. Monitor remediation records automatically generated through the ServiceNow Vulnerability Response (VR) module, participate in remediation meetings, and track deadlines, aging findings, and corrective actions. Support California Military Department security assessments and IRS audits by coordinating scan readiness, gathering technical evidence, validating security configurations, and tracking assigned findings through remediation. Escalate overdue or significant exposures and unresolved compliance deficiencies to the team lead and SOC Manager. Verify remediation through follow-up assessments and prepare reports on scan coverage, remediation progress, and outstanding vulnerability and compliance findings.

20 %	Zero Trust and Secure Access Support Support the administration of Zscaler Internet Access and Zscaler Private Access policies and other assigned secure access controls. Review Internet content filtering exception requests and access issues, analyze relevant logs, and implement approved policy changes in accordance with established procedures. Coordinate with security architecture, network, endpoint, and application teams to troubleshoot connectivity and access problems. Perform assigned Zero Trust implementation and testing activities, document configuration changes, and verify that approved controls operate as intended. Maintain troubleshooting guidance and provide backup support for secure access operations.
15 %	Cloud and Identity Security and External attack surface Monitoring Review cloud security assessments, identity exposure findings, and external attack surface monitoring results to identify vulnerabilities, misconfiguration, and potential exposures affecting DCSS information assets. Assist in analyzing findings related to cloud resources, identity platforms, Internet-facing systems, and exposed services. Coordinate with system owners and technical teams to validate findings, recommend corrective actions, and track remediation in accordance with departmental priorities. Support the administration of assigned monitoring tools, including maintaining settings, reviewing monitored assets, and validating asset ownership and attribution. Investigate findings, coordinate corrective actions with responsible teams, and submit supporting evidence to correct inaccurate findings as appropriate. Verify remediation through follow-up assessments, document progress, and escalate significant or unresolved exposures to the team lead and SOC Manager.

MARGINAL FUNCTIONS	
5 %	Represent the Information Security Office on special teams, projects, and other duties as assigned. Perform special assignments, attend meetings, and serve as back-up for peers. Invest in personal development and growth to maintain current knowledge in the IT field with emphasis on security services.
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 individual decisions and 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 down time, loss of business continuity, and poor customer service and performance.

B. Personal Contacts:
The incumbent has contact with CA DCSS managers, supervisors, and staff; State and LCSA staff; governmental 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:	