

DUTY STATEMENT

ASD 046 (REV. 03/2024)

Type of Duty Statement: Current & Proposed

Revision Date: 01/02/2026

1. Position Information			
A. Employee Name:			
B. Position Number:	C. CBID:	D. WWG:	E. Effective Date:
817-410-1415-001	M01	E	
F. Classification Title:		G. Working Title:	
Information Technology Specialist III		Principal CyberSecurity Architect	
H. Division:	I. Branch/Section/Unit:		
Technology Services	Enterprise Architecture & Security		
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 Branch Chief, an Information Technology Manager II (ITM II), in the Enterprise Architecture & Security Branch (EASB) of the Technology Services Division (TSD).			

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 expert advisor level. Under administrative direction of the Information Technology Manager II (ITM II), the Information Technology Specialist III (ITS III) serves as the Principal CyberSecurity Architect. The ITS III leads at an expert advisor level to continuously manage and improve Department of Child Support Services (DCSS) security posture in on-premises and on-cloud DCSS environments. The ITS III provides strategic and technical leadership, and mastery-level expertise to lead most complex projects to re-mediate IT security risks and ensures protection of the DCSS data and systems in the Enterprise Architecture & Security Branch, within Technology Services Division (TSD).	
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 %	CyberSecurity Architecture: Architects, designs, implements, and oversees overall DCSS security architecture to ensure securely designed DCSS systems, applications, and solutions. Leads the design and execution of the tactical security strategies and target DCSS CyberSecurity operating model. Evaluates security architecture and existing designs to determine adequacy and implements organizational requirement changes in support of Child Support program needs. Technical expert responsible to assess cloud, mobile, and other emerging technologies and implement security architecture improvements to ensure organization's confidential data is protected. Directs projects and coordinates duties to project personnel to implement proper security and privacy controls across on-premises and on-cloud DCSS infrastructure environments to effectively manage IT risks. Assume responsibility for implementation and maintenance activities of IT Security solutions, systems installation, operations, maintenance, repairs, and upgrades of IT Security appliances and infrastructure. Develops and documents DCSS CyberSecurity architecture road-maps and guidelines and ensure that the procured or developed systems align with security strategic directions and follow secure development practices. Develops IT Security architecture designs, models, and diagrams to accommodate multiple security classification levels of data (such as, Unclassified, Classified) and effectively communicates benefits, drivers, and merits of the architectural direction to the Information Security Officer, Chief Information Security Officer (CISO) and other stakeholders. Conducts and administers security and risk

20 %	CyberSecurity Policy & Compliance: Develops and leads the publication of the security policies, standards, and controls aligned with State, Federal, and DCSS requirements, and security industry best practices. Establishes IT Security and IT Risk policy governance models including security policy intake criteria, alignment with child support oversight agencies requirements, policy implementation prioritization, compliance processes, and risks assessment criteria. Undertakes development and review of compliance metrics, informs, and recommends management on the compliance gaps and risks, and guides TSD on the required changes to sustain confidentiality, integrity, and availability of organizational data, systems, and assets. Recommends new policies about sensitive and emerging data information and privacy risks to preserve the integrity of data security and privacy processes. Develops procedures to enforce compliance with security policies and requirements. Leverages available tools and technologies to inspect and administer security policies and procedures.
20 %	IT Risk Management: Develops and documents methodologies to evaluate IT Risks in alignment with IT Risk Governance framework. Performs security reviews, discovers gaps in the security architecture, and develops a security risk management plan. Leads and coordinates with IT Risk Committee to determine the measures to evaluate IT Risks and adjust IT Security project priorities based on IT Risks assessments and categorization. Contributes to the continuous governance, planning, development, assessment, and evaluation of the IT Risks to ensure adequate security for DCSS data and program. Guides the determination of potential threats and vulnerabilities for IT business processes, associated data, supporting capabilities, and in the evaluation of the enterprise risks. Develops an IT Risk awareness program and conducts trainings to ensure stakeholder awareness of the risks and to promote an IT risk-aware culture. Designs and implements IT controls in alignment with the IT Risk appetite and tolerance levels to support business goals. Develops metrics and key performance indicators to enable the measurement of effectiveness of implementing IT risk controls and support the business security requirements. Establishes and shares metrics with Information Security Officer, CISO, DCSS Executives and other stakeholders as appropriate to ensure DCSS' security posture efficacy against reducing CyberSecurity risks and the organization's resiliency against cyber threats. Monitors for emerging threats and recommends proper course of action to the Information Security Officer and the CISO. Documents and delivers regular and frequent communication, education, and reminders to Child Support staff of new security threats, best practices, policies, guidelines, and standards. Leads TSD to adopt secure coding, build, and deployment practices to ensure and mitigate supply chain, application security, and data security

20 %	Safeguard Auditing and Incident Response: Guides the incident response team in actively responding to the IT Security incidents and makes sound decisions to manage breaches, vulnerabilities, threats, and other security incidents to protect DCSS data, systems, and reputation. Builds partnerships with internal and external partners to lead incident investigations and responses. Solves complex security incidents, mediates discussions with internal teams, external government agencies, and vendor partners. Documents and relays security related matters and status reports into clear and understandable business terms to the Executives. Develops and steers procedures and processes to assess security policies, incident response plans, and analyzes their business impacts to ensure statewide compliance with DCSS, state, and federal security requirements. Travels to and oversees the physical and information security audits at the Local Child Support Agencies (LCSA) and contractor locations throughout California following applicable laws and regulatory requirements. Coaches team members on the auditing policies, procedures, and processes. Documents and presents audit findings to the management. Inspects the remediation plans and ensures audited entities implement prompt resolution of the audit findings. Liaisons with oversight agencies for information security audits conducted on DCSS by state and federal security oversight agencies to manage relationships and coordinate audit and findings remediation tasks. Facilitates IT Security Forums and shares security and risk updates to Information Security Officer, CISO, DCSS and LCSA Executives and staff.
0 %	N/A

MARGINAL FUNCTIONS

5 %	Assists Chief Information Officer (CIO), CISO, and other DCSS Managers & Supervisors in responding to initiatives. Maintains effective liaison with all levels of the DCSS Executives, management and staff, other public agencies, and the DCSS vendor community. Performs special assignments or projects for the Director's Office on matters dealing with risk and security. Represents EASB and TSD on special teams.
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 Local Child Support Agency 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:	