DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 046 (REV. 6/2021)

☐ **CURRENT**

☐ **PROPOSED** ☒ **CURRENT & PROPOSED**

Revision Date: 9/27/2021

1. POSITION INFORMATION

A. Position Number:	**B. Classification Title:**	**C. CBID:**
817-413-1414-MUL	Information Technology Specialist II	R01
D. Division:	**E. Branch/Section/Unit:**	**F. WWG:**
Technology Services	Enterprise Architecture & Security/Information Security/Information Security Architecture	E
G. Working Title:	**H. Employee Name:**	**I. Effective Date:**
Information Security Architect		Click or tap to enter a date.

2. POSITION REQUIREMENTS

A. Special Requirements: *Check All That Apply*

☒ Physical Requirements (Attach HSS 465-A)
☐ Bilingual Fluency (Non-English Language) – Specify Below
☒ Background Check Requirements
☐ Other – Specify Below

B. Special Requirements Description, as applicable: N/A

C. 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

Supervision Received:

The incumbent reports directly to the Information Technology Manager I in the Information Security Office.

4. DUTIES AND RESPONSIBILITIES OF THE POSITION

CONDUCT, ATTENDANCE AND PERFORMANCE EXPECTATIONS

This position requires the incumbent 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 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 (IT) information assets for the Department of Child Support Services (DCSS), Technology Services Division (TSD), Enterprise Architecture & Security Branch, Information Security Office (ISO), within the Information Security Architecture Unit.

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. ☐ Client Services ☒ Software Engineering ☒ Information Security ☒ IT Project Mgmt. ☒ System Engineering
35%	**Information Security Architecture:** Create Information Security Architecture (ISA) 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. Collaborate with Enterprise Architects to align ISA with Enterprise Architecture principles and policies; promote ISA business case by exposing benefits, drivers, and financial merits of the architectural direction; and help business users realize savings and rational investment decisions. Define roadmaps to help establish the ISA program to align with DCSS vision and objectives. Manage alignment of DCSS program decisions to ISA roadmaps by working with DCSS Leadership team and Enterprise Architects to ensure continued progress and compliance with DCSS objectives. 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 systems security design and recommend enhancements. Coordinate with DCSS and Local Child Support Agency (LCSA) 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. Lead meetings, workgroups, 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.
25%	**Safeguard Auditing and Incident Response:** Serve as the lead in the development and maintenance of procedures and processes to assess security policies and analyze their business impacts via audits to ensure statewide compliance with departmental, state, and federal security requirements. Travel to and lead physical security audits at LCSAs and provide findings reports to ensure DCSS information is protected as required. Act as DCSS ISO point of contact for information security audits conducted by departmental, state, and federal security oversight agencies to ensure audits are efficiently coordinated. Track findings from the audits and coordinate and monitor the resolutions of the findings to ensure findings are remediated.

	Lead the development and maintenance of procedures to monitor and investigate information security events. Respond to information security incidents and lead and mentor staff who are responding to information security incidents. Provide consultation and direction to LCSAs in the implementation of information security practices and respond to requests for information security direction to ensure statewide compliance with state and federal security requirements.
15%	**Business Continuity Planning:** Lead the development, management, and maintenance of the DCSS Business Continuity Plan (BCP) to ensure the continuance of the Child Support Program during times of emergency or disaster. Conduct preliminary planning, perform business impact analysis, define business continuity processes and priorities, and identify business continuity contingency organizations, key stakeholders and decision makers needed to implement the BCP and ensure it meets the needs of the Department. Seek approval from oversight agencies on Business Continuity and coordinate plans and tests across the counties to ensure statewide Business Continuity, site readiness and business operations are maintained at the required level during an emergency. Lead testing and training exercises to ensure the efficacy of the BCP and guide revisions to the BCP as warranted. Coordinate the BCP with the Technology Recovery Plan developed and maintained by the Infrastructure Branch team to ensure plan consistency.
10%	**Policy Development and Information Security Awareness:** 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 Manual (ISM) and develop ISO policies. 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.
10%	**Information Security Monitoring:** Serve as lead in the monitoring and analysis of static code scans, web application scans and server and network compliance scans for the identification of abnormal behavior and potential vulnerabilities. Perform raw packet data analysis to determine if network security policies are being followed. 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.
MARGINAL FUNCTIONS	
5%	Assist ITM I, Chief Information Security Officer, Lead Enterprise Architect, other TSD Branch Chiefs, and Chief Information Officer 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 ISO staff. Invest in personal development and growth to maintain current knowledge in the IT field with an emphasis on security services.

5. WORKING ENVIRONMENT AND CONDITIONS

Two story building with standard office workspace. Requires sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings in designated areas. The position requires occasional travel to off-site meeting locations, conferences, or training. The work environment is fast paced and requires the incumbent to be flexible, use good

time management practices, and effectively identify priorities to complete assignments timely. May require periodic work during non-standard hours and during weekends to meet workload needs.

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 LCSA 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 Wellness and Safeguards Unit.

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:	