DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 045 (REV. 6/2021)

☐ CURRENT

☒ PROPOSED ☐ CURRENT & PROPOSED

Revision Date: 2/16/2022

1. POSITION INFORMATION

A. Position Number:	**B. Classification Title:**	**C. CBID:**
817-410-1415-001	Information Technology Specialist III	M01
D. Division:	**E. Branch/Section/Unit:**	**F. WWG:**
Technology Services	Enterprise Architecture & Security	E
G. Working Title:	**H. Employee Name:**	**I. Effective Date:**
Principal Cybersecurity 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

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).

B. Supervision Exercised:

None

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 the broad administrative and policy 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 as 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 remediate IT security risks and ensures protection of the DCSS data and systems. The duties for this position focus in all six domains: Business Technology Management, Information Security Engineering, Client Services, Information Technology Project Management, Software Engineering, and System Engineering.

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%	**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 roadmaps 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 assessments through penetration and vulnerability testing to set up an effective security compliance testing program. Serves as the subject matter expert across multiple security domains, such as network, endpoints, systems, and applications, to lead TSD staff on the security and risk strategy in the cloud and on-premises environments. Assesses security controls and documents the gaps and protection needs for DCSS systems, networks, and applications. Researches and presents emerging IT Security related trends, tactics, vendors, and solutions to Information Security Officer and CISO and recommends proper course of action to improve DCSS security posture.
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 risks throughout the software development life cycle.
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.

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, projects, and in other duties as assigned. Responds to written and verbal inquiries from DCSS Executives and external parties on security, risk, disclosure, or resolution management issues. Performs special assignments, attend meetings, and serves as backup for ISO staff. Invests 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 modular workspace. Requires sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings/trainings, etc., in designated areas. Requires occasional travel to off-site meeting locations, conferences, or training. 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 and/or to support staff who work during these hours.

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.

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

N/A

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:	