DEPARTMENT OF CHILD SUPPORT SERVICES

DUTY STATEMENT

ASD 046 (REV. 03/2024)

Type of Duty Statement:	Current & Proposed	**Revision Date:**	02/13/2025

1. Position Information

A. Employee Name:

B. Position Number:	**C. CBID:**	**D. WWG:**	**E. Effective Date:**
817-411-1414-004	R01	E	

F. Classification Title:	**G. Working Title:**
Information Technology Specialist II	Insider Threat Security Engineer

H. Division:	**I. Branch/Section/Unit:**
Technology Services	Enterprise Architecture and Security Branch/Risk & Privacy Office

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 Risk & Privacy Office.

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 general direction of the Risk & Privacy Office Information Technology Manager I (ITM I), the Information Technology Specialist II (ITS II) is responsible for providing a variety of expert-level risk management services to the Department, Division's project teams and senior management. These services include the development, implementation, oversight and management of Enterprise Insider Threat program in the Risk & Privacy Office, Enterprise Architecture & Security Branch, within the 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
30 %	Threat Identification and Analysis: Performs technical and analytical research to support the development, documentation, and communication of Department of Child Support Services' (DCSS) risk assessment methodology, including the identification, quantification, and prioritization of Insider threats and risks. Establish controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. Create alerts and checks to ensure data integrity within the Child Support Program. Develop queries in log data to find signs of insider threat activity to include stolen credentials, compromised accounts/systems, potential fraud. Creates queries to various logs sources and systems using Cortex Query Language, Kusto Query Language, and Structured Query Language to analyze huge data sets to find evidence of Insider Threat activity.

30 %	Threat Monitoring: Conduct host-based user monitoring of individual employee activities on government-owned computers. Monitor caseworker identities and millions of participant identities for the following risks: Careless User, Malicious User, Compromised Credentials. Regularly review caseworker activities and create threat hunts off found anomalous activity. Regularly review case recusals and high-profile cases statewide for caseworker and administrator activity and compare caseloads to cases viewed for caseworkers statewide. Examine employee records, background checks, and case recusals to build insider risk profiles. Activities to be monitored by the Insider Threat Program include the following: fraud (caseworker, financial, participant); data theft by compromised credentials, machines, and identities; and system sabotage of the largest Child Support Enforcement (CSE) program in the nation. Conduct threat analysis and self-assessments of the DCSS's insider threat posture. Maintain an Insider Threat Risk Register to track and monitor all suspected threats across the enterprise.
25 %	Threat Investigation: Investigate anomalous log in activity for participants of the Child Support Program. Investigate anomalous case activity within the Child Support Program and anomalous financial activity through the State Disbursement Unit. Conduct and manage an enterprise fraud program to include, case worker fraud. Develop fraud profiles for internal and external users to the child support program and transform that fraud into actionable alerts and risk profiles. Conduct active and automated fraud investigations within the Child Support Program. Conducts and supports HR and Legal-initiated investigations related to potential insider threats, policy violations, and misuse of IT systems. Support legal teams in responding to subpoenas, e-discovery requests, or regulatory audits related to insider threat cases. Prepares reports on agreed upon recommendations and findings for executive-level management.

15 %	Threat Training and Prevention: Develop insider threat training and polices and implementation plans for the department. Provide insider threat awareness training to employees. Independently prepares both written and oral reports on program-level risk exposure, residual risk ratings and current mitigation efforts for the DCSS executive-level management, and senior management. Develop Fraud Manual. Institute regulatory and compliance requirements. Establishes and maintains a research function by developing research protocols and procedures for collecting, analyzing, and publishing a variety of Insider Threat Management related data and articles.
0 %	N/A

MARGINAL FUNCTIONS	
5 %	Provides overall support to the Branch IT Manager II, Chief Information Officer, Chief Information Security Officer, and staff as the expert in Insider Threat and Risk Management topics. Represents TSD on special teams, projects, and other duties as assigned. Performs special assignments, attend meetings, and serve as back-up for the Section Manager and peers as needed.
105 %	**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 management and 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:	