STATE OF CALIFORNIA
CALIFORNIA DEPARTMENT OF AGING
DUTY STATEMENT
CDA 9003 (REV 02/2024)

☐ Current
☒ Proposed

Civil Service Classification:	Information Technology Specialist II
Working Title:	Assistant Information Security Officer
Division Branch Name:	Information Security Branch
Incumbent:	Vacant
Position Number:	797-910-1414-950
Effective Date:	
Conflict of Interest (COI):	Y
FLSA Status:	Non-Exempt
CBID:	R01
Tenure:	Permanent
Time Base:	Full Time

You are a valued member of the department's team. All CDA employees are expected to work collaboratively with internal and external stakeholders to enable the department to provide the highest level of service possible. Your efforts to treat others fairly, honestly, and with respect are important to everyone who works with you. We value diversity at CDA and we strive to achieve equity and inclusion in the workplace for all employees. We believe that a diverse workforce and inclusive workforce workplace culture enhances the performance of our organization and the quality of representation that we provide to a diverse client base.

Primary Domain(s): Information Security Engineering

DESCRIPTION:

Under the general direction of the Information Technology Manager I (ITM I) Information Security Officer (ISO), the Information Technology Specialist II (ITS II) serves as a cybersecurity advisor and provides technical security expertise to the ISO as the Assistant Information Security Officer (AISO). The AISO implements and maintains security governance and the associated frameworks and processes. The AISO serves a critical function in the development, implementation, and maintenance of cybersecurity policy training. Other key functions include risk and compliance management, incident response and technology recovery testing and planning; evaluation and implementation of security controls; audit planning and reporting; security assessments; supporting the Department's security awareness training platform and processes; and developing and sustaining cooperative working relationships with all stakeholders.

ESSENTIAL JOB FUNCTIONS:

35% **IT Security Governance**:

Leads the development, implementation, and maintenance of the IT security governance framework and processes for CDA. Assists the ISO in developing and refining the IT security governance structure and associated committees. Oversees and collaborates with peers in the development, improvement, review, and implemention of security policies, standards, plans, and procedures to mitigate risk to CDA data, systems, and physical/electronic assets. Recommends, coordinates, and communicates security policies, standards, and procedures to protect CDA's information and data assets. Develops and oversees a document framework for keeping up-to-date cybersecurity policies, standards, and guidelines. Provides regular reporting on the status of CDA's security posture to the ISO, technical teams, and business leaders. Works collaboratively with technical leads and CDA staff to ensure cybersecurity requirements are incorporated into CDA contracts and procurement processes. Reviews contracts and project plans to ensure compliance with CDA and Division of Information Technology (DIT) security policies, standards, plans, and procedures. Interacts with technical teams and diverse CDA staff to ensure consistent application of cybersecurity policies and standards across all IT projects, systems and services, risk management, compliance, and business continuity.

30% **Risk and Compliance:**

Provides recommendations to improve the cyber risk posture of CDA including the prevention and mitigatation of security risk which includes the application of controls. Plans, manages and coordinates regular compliance reviews and risk assessments to ensure compliance with CDA and state requirements, policies, and standards. Explores, develops, and recommends strategies and remediation plans to mitigate identified risks. Evaluates cybersecurity tools and technologies to implement security controls within acceptable risk thresholds. Maintains compliance documentation and records to stay up-to-date on compliance issues and trends. Communicates cybersecurity risks and compliance requirements to senior management and stakeholders including trainings to educate employees on cybersecurity compliance requirements. Collaborates with business leaders to balance the need for security requirements with the operational need for agility, innovation and growth. Performs security reviews to identify gaps in security architectures and to make recommendations for CDA's overall risk mitigation strategy. Works collaboratively with stakeholders to communicate business risk and risk mediation by providing viable secure options to mitigate the risk.

20% **Security Incidents and Technology Recovery:**

Assists with the planning, development, review, maintenance and testing of the Technology Recovery Plan as required by state policy. Leads and facilitiates CDA disaster recovery exercises. Serves as the back-up to the ISO in Agency and State level Technology Recovery Coordinator meetings, forums, training, surveys, and committees. Assists the ISO in planning and responding to security incidents and audit findings to protect CDA data and information assets. Leads, manages, and oversees the investigation and documentation of Information Security Incidents by providing technical guidance to IT teams to identify root cause and resolve security incidents. Provides timely and relevant updates to appropriate stakeholders and decision makers. Communicates investigation findings to relevant business units and IT leadership to help improve CDA's security posture. Coordinates the development of incident

response plans and procedures to identify potential threats. Compiles and analyzes data for the ISO related to reporting and metrics. Conducts research and stays up to date on the latest security trends, tools, and methods to retain a current understanding of security threats and trends. Develops procedures to incident handling, particularly for analyzing incident-related data and determining the appropriate response. Maintains logs and prepares, coordinates, and submits all security related incident reports. Analyzes Information Security incidents to advise on appropriate corrective actions related to the incident management and process improvement.

10% **IT Security Liaison and Coordinator**

Liaises with external oversight entities to ensure CDA meets state and federal security requirements. Coordinates with technical teams to plan and implement security controls and measures to identify and mitigate security threats and vulnerabilties. Ensures cybersecurity requirements are built into architectures and designs for all IT work. Attends State ISO and Agency ISO meetings on behalf of the CDA ISO as directed. Participates in various internal and external workgroups, committees, and various meetings and discussions requiring an Information Security perspective or consultation. Assists the ISO with cybersecurity related budgeting, auditing, and reporting activities. Responsible for managing the security awareness training platform, exercises, and associated processes to ensure CDA staff complete annual security awareness training requirements.

MARGINAL JOB FUNCTIONS:

5% Performs other job-related duties, special assignments, and projects as required in order to fulfill the mission, goals and objectives of the Division of Information Technology and the needs of the department.

TRAVEL: Not Required

TYPICAL WORKING CONDITIONS:

The physical work location of the position is designated at the department's headquarters location, a three-story building and standard office modular workspace located in Natomas. The duties of the position require sitting for long periods of time while using a personal computer, reviewing documents, and attending meetings whether they are digital (i.e., Zoom, WebEx, MS Teams, etc.) or in person.

EQUAL EMPLOYMENT OPPORTUNITY:

The California Department of Aging is an equal opportunity employer to all, regardless of age, ancestry, color, disability (mental and physical), exercising the right to family care and medical leave, gender, gender expression, gender identity, genetic information, marital status, medical condition, military or veteran status, national origin, political affiliation, race, religious creed, sex (includes pregnancy, childbirth, breastfeeding and related medical conditions), and sexual orientation.

It is the policy of CDA to provide equal employment opportunity to all employees and applicants; those employees have the right to work in an environment free from discrimination; those consumers

have the right to receive services free from discrimination in compliance with local, state, and federal laws.

To be reviewed and signed by the supervisor and employee:

SUPERVISOR'S STATEMENT:

- I have discussed the duties and responsibilities of the position with the employee.
- I have signed and received a copy of the duty statement.

_____ _____

Supervisor's Signature and Date **Supervisor's Name and Title**

EMPLOYEE'S STATEMENT:

- I have discussed the duties and responsibilities of the position with my supervisor.
- I have signed and received a copy of the duty statement.
- I am able to perform the essential functions listed with or without reasonable accommodation (if you believe reasonable accommodation is necessary, discuss your concerns with your supervisor. If unsure of a need for reasonable accommodation, inform your supervisor who will discuss your concerns with Human Resources.)
- I understand that I may be asked to perform other duties as assigned within my current classification, including work in other functional areas as business needs require.

_____

Employee's Signature and Date

HUMAN RESOURCES BRANCH USE ONLY:

☒ Duties meet class specification and allocation guidelines.

☐ Exceptional allocation, STD 625 on file.

Analyst initials: LD Date Approved: 12/12/24

Revision Date (if applicable): _____