Duty Statement
California Government Operations Agency
State of California

☒ Current ☒ Proposed

Classification Title Information Technology Manager II	**Division** Data Infrastructure
Working Title Chief Information Security Officer	**Office/Unit/Section** Office of Cradle-to-Career Data
Position Number 424-100-1406-900	**Effective Date**
Name	**Date Prepared** 9/18/23

General Statement

The Office of Cradle-to-Career Data (C2C) is building a statewide longitudinal data system that will provide policymakers, researchers, educators, students, families, and other stakeholders answers to key questions about student progression and outcomes. The data system will help provide critical information about the pipelines from early care to K-12 to higher education skills training and employment along with health and human services data. This data system will help support teachers, advisors, parents and students and be an evidence-based tool that decision makers and researchers can use to help California adopt more equitable policies by providing insight into how educational experiences impact students' subsequent academic achievement, work, and earnings.

Under the administrative direction of the Director of Data Infrastructure (CEA C) the Information Technology Manager II (ITM II) serves as Chief Information Security Officer (CISO) for the longitudinal data system itself as well as the C2C office.

Specific duties include, but are not limited to:

Job Functions

[Essential (E) / Marginal (M) Functions]:

50% (E) CISO, C2C Data System

- Oversee the collaboration efforts between C2C state staff and consultant(s) and the System Integrator (SI) staff in the development of C2C Data System Deliverable Expectations Document (DED) for each information security related Deliverable throughout all phases of the C2C System Development Life Cycle (SDLC).
- Approve information security related SI DEDs.
- Review and grant approval of each security related SI Deliverable throughout all phases of the C2C Data System's SDLC.
- Ensure and certify all functional and non-functional security related RFP requirements are met for each phase of the C2C Data System's SDLC and before any component of the C2C Data System goes into production.
- Approve all test plans for execution.
- Oversee state staff and consultant(s) efforts to validate hundreds of mandatory security related functional and non-functional requirements.
- Manage and report to the C2C Office executive team and the C2C Data System Project stakeholders on security risks and issues throughout all phases of the C2C Data System SDLC, including oversight of the SI's performance and timely handling of the C2C Data System risk and issue log.
- Approve satisfactory SI security related Deliverables prior to release of any payment.
- Ensure knowledge transfer from SI to state staff.
- Ensure timely requests for adequate funding for C2C state staffing and tools to ensure System security and resilience.
- Manage security incidents throughout the Data System's SDLC, including compliance with all federal and state regulatory requirements for breach notification and resolution.
- Manage suspected and confirmed security incidents in Cal-CSIRS.
- Manage the access by all authorized state C2C staff to control agency information resources, including Cal-CSIRS, SAFE, and AgencyNet.
- Manage the C2C Plan of Action and Milestones (POAM), including quarterly and annual updates of SIMM 5330-C to C2C Director and California Department of Technology (CDT) Office of Information Security (OIS).
- Ensure time sensitive compliance reporting to CDT OIS, including the following:
    - Designation Letter SIMM 5330-A
    - Information Security and Privacy Program Compliance Certification SIMM 5330-B (this includes SIMM 5330-C POAM Excel workbook)
    - Technology Recovery Program Certification SIMM 5325-B (includes filing of the C2C Office Technology Recovery Plan and evidence of successful testing)
    - Host/Hosted Entities SIMM 5330-E
- Ensure timely annual reporting of health-related security incidents/breaches to California Office of Health Information Integrity (Cal-OHII).

- Direct the Security Consultant and the System Integrator's Security lead to develop and manage C2C Data System Security Plan.
- Facilitate all federal, state, and industry audits and ensure all audit findings of security risks are properly managed in the C2C Risk Register and reported on via SIMM 5330-C.
- Build and maintain adequate cybersecurity security workforce.
- Build and maintain a cooperative relationship with all C2C Data System stakeholders.
- Develop and maintain security policies and procedures in support of the C2C Information Security Program.

50% (E) CISO, C2C Office

- ***Information Security Strategic Planning and Policy Management (10%)***
    - Under the administrative direction of the Director of Data Infrastructure, serve in an executive management role in setting the organizational information security strategy and policy and in formulating the long-range information security program objectives.
    - Collaborate with the State Chief Information Security Officer (CISO) to ensure C2C's information security strategy and policies align with statewide information security initiatives.
    - Serve as the direct interface with the State Office of Information Security (OIS) on all information security policy matters; represent C2C on security policy and standards workgroups.
    - Develop, implement, and maintain information security policies, standards, guidelines, processes, and procedures in accordance with the department's strategy, State Administrative Manual, OIS policies and guidance, and other applicable state and federal regulations.
    - Direct the maintenance and enforcement of security policies, and standards to safeguard C2C system, data, interfaces, and C2C's information processing infrastructure.
    - Establish cooperative relationships with management, data owners, data custodians, and information users.
    - Ensure that the security policies and procedures are reviewed and updated as needed to prevent new threats and vulnerabilities. The policies and procedures must address data for all media types (electronic and paper) and provide detailed processes in how to handle the data.
    - Research and evaluate current and new information security technology and trends to develop C2C's information security strategic plan and roadmap.
    - Collaborate with C2C's infrastructure and application development teams to manage the design and implementation of information security technical controls and/or threat counter-measures.
    - Manage Information Security Governance to ensure alignment of information security objectives with the business strategy, optimized security investments and measurable results.
    - Conduct analysis and prepare reports related to information security trends and best practices in order to be continuously prepared for improving the C2C security posture,

utilizing inputs from staff, clients, peers and independent research in accordance with the direction of the Director of Data Infrastructure and C2C's executive management.

- ***Information Security Program and Risk Management (10%)***
    - Provide strategic direction and lead the development, implementation, and management of a comprehensive information security program to support and align the C2C system and the office's information processing infrastructure with the department's mission, goals, and objectives.
    - Protect the C2C data system and the office's information and information processing assets with effective security controls.
    - Strategically manage the vulnerabilities, threats and incidents impacting the C2C data system and the office's information resources; direct the development and implementation of mitigation strategies.
    - Oversee the implementation of an effective information security risk management program covering risk assessment, mitigation, and evaluation.
    - Lead the oversight efforts for technology recovery planning and participate in the testing and documentation of issues and resolutions.
    - Direct security audits reviews for all major systems and data processing activities to ensure compliance with laws, statutes, regulations and C2C security policies.
    - Lead the development of responses to audit findings, plan actions and milestones to address the findings, and oversee the implementation of planned actions to address the findings.
    - Ensure departments/staff are following the appropriate policies in regard to the appropriate use of the office's information resources.
    - Ensure staff are educated on information security and privacy protection responsibilities; ensure security training is provided to all C2C staff on at least an annual basis.
- ***Access Control, Governance, Risk, and Compliance (10%)***
    - Control and manage access, using the principle of "least privilege" to the office's IT assets to ensure that only authorized devices/persons have access as is appropriate in accordance with the business needs.
    - Collaborate with the office's infrastructure and application development teams and ensure that security properly integrates with the system and software development lifecycle and that security requirements including the capture of adequate information for auditing are effectively addressed.
    - Develop enterprise-level security analytics strategy and oversee the implementation of the analytics program for transactional and access control governance.
    - Implement, direct and manage the data capture and analysis activities to detect potential fraud and exposure; identify solutions and coordinate their implementation to prevent fraud and exposure.
- ***Security Infrastructure Operations (10%)***
    - Direct and manage the design, development, implementation, and ongoing support of information security tools including the Identity and Access Management (IdAM) solution components.
    - Direct and manage the design, development, implementation and ongoing support of Security Information and Event Management (SIEM) solution components.

- Collaborate with the C2C Data Infrastructure team to implement and operate industry-strength tools and technologies for endpoint protection, perimeter defense, malware defense, intrusion prevention, and other preventative controls.

- **Administrative (10%)**
  - Prepare budget estimates and recommendations for procurement of services, training, and necessary information security software and services.
  - Proactively manage information security spending and implement solutions to reduce operational costs in order to create budget for innovative applications.
  - Maintain currency with security technologies, policies, and standards. Attend training classes as needed. Satisfactorily complete all team-training requirements.
  - Perform other related duties as required to fulfill C2C's mission, goals, and objectives.

Supervision Received

The incumbent reports directly to and receives the majority of assignments from the Director of Data Infrastructure. Assignments may also come from the Executive Director.

Supervision Exercised

The Chief Information Security Officer will not exercise any formal supervision; however, they will provide project and program leadership and functional guidance to state staff and contractors.

Personal Contacts

The incumbent will work with teams across the Office of Cradle-to-Career Data and GovOps Agency staff, community organizations, a wide range of stakeholders, and external contractors and advisors.

Actions and Consequences

The incumbent's duties are critical to the successful implementation of Data Infrastructure for the highly visible C2C program. Inadequate performance by the incumbent may affect or compromise C2C's ability to accept data from its data sharing providers and keep it secure.

Functional Requirements

The demands described here are representative of those that must be met by the incumbent, with or without a reasonable accommodation, to successfully perform the essential functions of the job:

- Regular and consistent attendance is essential to the successful performance in this position.
- The ITM II is expected to be prepared and professional and must be flexible in terms of work hours.
- Requires daily use of a personal computer and related software applications at a workstation.
- Requires ability to complete tasks that typically may require making repetitive hand movements in the performance of daily duties, with or without reasonable accommodations and modifications to facilitate such tasks.
- Requires occasional travel to attend meetings and hearings.

The office environment is in a high-rise building under fluorescent lighting with sufficient temperature control, in close proximity with other employees and utilizes typical office equipment, such as

telecommunications equipment, computers, and photocopiers/scanners. Standing, bending, walking, and stooping are required.

Background Checks and Clearance

The successful candidate will be required to pass a criminal background check (see Education Code 10873).

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. (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 discuss your concerns with the Personnel analyst.)
Duties of this position are subject to change and may be revised as needed or required.

Employee Signature	**Employee Printed Name**	**Date**

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

Supervisor Signature	**Supervisor Printed Name**	**Date**