Duty Statement
California Government Operations Agency
State of California

☐ Current ☒ Proposed

Classification Title	**Division**
Information Technology Manager II	Data Infrastructure
Working Title	**Office/Unit/Section**
Chief Information Security Officer	Office of Cradle-to-Career Data
Position Number	**Effective Date**
424-100-1406-004	
Name	**Date Prepared**
Vacant	3/27/26

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]:

35% (E) Security Architecture and Engineering

- Manage C2C security staff/consultants during the System Development Life Cycle (SDLC) for each information security related deliverable; approve/reject information security deliverables throughout all phases of the SDLC.
- Manage the design, documentation, implementation, and continuous operation of security technologies including SIEM for monitoring, EPP/EDR for malware defense, IDS/IPS for intrusion detection and prevention, and DLP for protection of sensitive and proprietary information from theft, misuse, or accidental disclosure.
- Collaborate with infrastructure/platform and application teams to integrate security controls into the SDLC.
- Review architectural diagrams before and after any system changes/enhancements.
- Manage security testing (SAST, DAST, Penetration Testing, etc.) during the SDLC; review rules of engagement, deployment gates, and test results.
- Manage the System Security Plan (SSP); provide SSP status updates to internal and external oversight bodies upon request.
- Ensure all functional and non-functional security related requirements are met for each phase of the SDLC and before any component is promoted to production.

35% (E) Security Program and Governance

- Set the enterprise information security vision, strategy, program objectives, and roadmap aligned with departmental mission, statewide policies (SAM, SIMM), and federal standards (NIST).
- Develop, implement, and maintain information security policies, standards, guidelines, and procedures; ensure consistent governance and enforcement across the department.
- Serve as the principal policy liaison with statewide security authorities (Agency and State CISOs, CDT OIS); represent the department in security matters for governing boards, advisory boards, task forces, and workgroups.
- Lead a comprehensive information security program that includes risk assessment, mitigation, evaluation, and continuous improvement; manage the Risk Register and Plan of Action and Milestones (RR-POA&M).
- Ensure compliance with applicable U.S. and California statutes, regulations, policies, standards, and frameworks (e.g., FERPA, HIPAA, SAM, SIMM, NIST, ISO/IEC).
- Facilitate internal and external assessments, audits, and enterprise technology recovery plan testing; file required security and recovery reports with control agencies.
- Manage progress toward higher maturity levels for Zero Trust Architecture.

10% (E) Identity, Access, and Data Protection

- Implement and manage Identity and Access Management (IAM) controls and processes; enforce the least-privilege principle and access governance across systems and data.

- Conduct periodic reviews of access control, and identification and authentication documentation (e.g., Separation of Duties Matrix).
- Develop enterprise security analytics for transactional and access control governance; detect and prevent fraud/exposure through data capture and analysis.

5% (E) Incident Response and Technology Recovery

- Maintain the Cybersecurity Incident Response Plan (IRP); lead incident response efforts of detection, investigation, containment, eradication, recovery, reporting, and post-incident reviews.
- Collaborate with the infrastructure team on technology recovery planning and testing; ensure alignment with business continuity programs and statewide requirements (SAM, SIMM).

5% (E) Staff Leadership and Development

- Plan, organize, and direct the workload for C2C security staff/consultants; hire, mentor, develop, and retain a high-performing security workforce; monitor performance and deliver services to organizational standards.
- Provide security awareness and training programs for staff; promote a culture of security and accountability.

5% (E) Budgeting, Procurement & Resource Stewardship

- Prepare budget estimates and procurement recommendations for security tools and services; optimize operational costs; ensure effective use of resources.

5% (M) External Coordination & Representation

- Coordinate with control agencies (California Department of Technology Office of Information Security), auditors, law enforcement, regulated entities, counties, vendors, and partner departments; represent the department in statewide initiatives.

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.

The duties of this position are performed indoors. C2C Headquarters is located at 400 R Street, Sacramento, CA 95811 and is equipped with standard or ergonomic office equipment, as appropriate. A hybrid work schedule is acceptable pursuant to an approved Telework Agreement. Additionally, occasional travel and overnight stays may be required to attend meetings, conferences, and training.

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**