POSITION DUTY STATEMENT

California Student Aid Commission
State of California

☐ Current

☒ Proposed 10/13/2025
Date Revised

Date: October 13, 2025	**Name of Incumbent:** Vacant
Civil Service Title: Information Technology Manager I	**Position Number:** 270-701-1405-XXX
Working or Job Title: Chief Information Security Officer	**Division/Unit:** ITSD/Information Security Office
Supervisor's Civil Service Title: Career Executive Assignment—Level B	**Location:** Rancho Cordova
Supervisor's Working Title: Deputy Director/Chief Information Officer	**Work Hours/Shift:** 8:00 a.m-.5:00 p.m./M-F
Conflict of Interest Disclosure Position: ☒ Yes ☐ No	**License or Other Requirement:** N/A
Bilingual Position (Specify Language): ☐ Yes _____ ☒ No	**Public Contact Position:** ☐ Yes ☒ No

Supervision Exercised: You serve as the Chief Information Security Officer and supervise 1.0 Information Technology Specialist II, 1.0 Information Technology Specialist I, and 1.0 Information Technology Associate.

This role is critical to accomplishing CSAC's established goals to advance equitable student access, support and success and you are a valued member of the California Student Aid Commission's (CSAC) team. You are expected to work cooperatively with team members and others to enable CSAC to provide the highest level of service possible. Your creativity and productivity are encouraged. Your efforts to treat others fairly, honestly, and with respect are important to everyone who works with you.

CSAC MISSION STATEMENT

CSAC is the principal state agency responsible for administering financial aid programs for students attending public and private universities, colleges, and vocational schools in California. Its central mission is to make education beyond high school financially accessible to all Californians.

PROGRAM INFORMATION

The Information Technology Services Division (ITSD) is an enthusiastic team of IT professionals who play a critical role in assuring the Commission's ability to promote educational equity by making post-secondary education affordable for all Californians. We are comprised of multiple teams including application developers, database administrators, network and server administrators, cybersecurity professionals and more. We accomplish these lofty goals by safeguarding student data while creating and maintaining customer-minded applications, that are easy to use based on modern, scalable technology that forms the backbone of our operations.

SUMMARY STATEMENT
Under the general direction of the Career Executive Assignment-Level B, Deputy Director/Chief Information Officer (CIO) within the ITSD, the Chief Information Security Officer (CISO)/IT Manager I serves as both a strategic leader and hands-on technology professional responsible for the direction, oversight, and operation of the CSAC Information Security Office (ISO). This managerial-level position provides expert consultation on complex information security practices and supervises a diverse team of information security professionals, technical staff, and contract personnel with varying skill sets. The incumbent is responsible for developing and implementing information security policies and operational standards; managing incident response, risk assessment and mitigation, investigations, litigation support, data privacy and classification, continuity planning, audits, and assessments; and ensuring compliance with applicable laws, Government Code, and State Administrative Manual (SAM) requirements. The incumbent also analyzes security-related budget change proposals, provides guidance and technical assistance to executive management, and serves as the liaison to control agencies for communicating security policies, incident responses, and action plans. The CISO/IT Manager I co-leads projects to assess risk exposure, monitors threats and vulnerabilities, and conducts annual security and privacy training for all employees. Success in this role requires strong leadership, communication, and customer service skills, with the ability to foster a collaborative, motivated, and informed workforce while working closely with internal program partners, external vendors, and oversight agencies.

ESSENTIAL FUNCTIONS (E) – MARGINAL FUNCTIONS (M)	
%	**Job Descriptions**
30% (E)	Responsible for establishing, developing, implementing, and maintaining a comprehensive Information Security Program in compliance with SAM 5300 (Information Security), SIMM 5300 (Information Security), and Cal-Secure. This includes developing all necessary security policies, standards, and procedures to ensure the confidentiality, integrity, and availability of CSAC's information assets. Oversees the strategic direction, vision, and program management of the CSAC ISO, aligning information technology security initiatives with enterprise programs and CSAC objectives to adequately protect information assets and technologies. Supervises, plans, organizes, and directs the work of the ISO, providing operational guidelines and oversight to integrate appropriate security protocols into new or enhanced IT environments and systems. Responsible for the design, development, implementation, and operation of information security and privacy programs covering the collection, use, storage, and destruction of information assets. Ensures that all security and privacy policies and procedures are followed, including the delivery of security and privacy awareness training to employees, conducting periodic phishing exercises, and disseminating quarterly security awareness notices. Monitors compliance with State information security policies, coordinates annual compliance reporting with control agencies, and represents CSAC in statewide security policy and standards workgroups, technology forums, conferences, and audits. Provides oversight of IT security applications, practices, and standards pursuant to SAM and NIST guidelines, reviews and approves changes involving confidential and sensitive data, and leads efforts to resolve audit findings. Conducts security risk assessments and analyses to identify critical assets, vulnerabilities, and the adequacy of security safeguards. Develops policies, procedures, and solutions to implement Zero Trust Architecture and ensures all departmental employees participate in required training and adhere to established policies and procedures.

25% (E)	Responsible for the administration, operation, and internal program management of the CSAC ISO, including the management and supervision of staff. Plans, organizes, directs, and administers the workload and activities of ISO resources, evaluating the effectiveness of staff and developing performance measures. Establishes and communicates performance standards and expectations, conducts probationary reviews, annual performance appraisals, individual development plans, and implements constructive interventions, corrective, and disciplinary actions as needed. Assigns workload, sets reasonable deadlines, and monitors progress while providing guidance and consultation on complex and sensitive work issues. Develops training plans to ensure continuous improvement and enforces systems, policies, procedures, and productivity standards. Designs long-and short-term plans to address information security risks and strengthen the organization's security posture. Monitors compliance with established plans, schedules, directives, and procedures to ensure quality of services through rigorous oversight practices. Serves as a back-up to the CIO.
20% (E)	Establishes and leads an Incident Management Program and develops appropriate security-incident notification procedures. Develops and manages CSAC's cybersecurity incident response plans and directs regular tabletop exercises to ensure organizational cybersecurity incident response readiness. Ensures that lessons learned and findings from tabletop exercises are addressed and remediated. Manages cybersecurity threats and incidents affecting CSAC information assets and technology resources, overseeing efforts in cybersecurity incident investigation, digital forensics, and system recovery. Ensures digital forensics capabilities support legally defensible preservation of data in adherence to industry-standard best practices. Determines the authenticity of reported security violations, reviews security incident reports, and provides incident reports to executives, State Control Agencies, the California Highway Patrol (CHP), and the Emergency Notification and Tactical Alert Center (ENTAC) per SIMM 5340-A. Coordinates forensic investigative matters with all appropriate agencies. Conducts post-incident reviews, develops action plans to reduce further exposure, and evaluates and reports on trends and weaknesses in the security program. Actively participates on CSAC committees for Continuity Planning, Technology Planning, and in the coordination of tabletop and recovery exercises.
15% (E)	The incumbent is responsible for conducting comprehensive cybersecurity and privacy risk management activities across all departmental systems, applications, and business processes. This includes performing ongoing risk assessments to identify vulnerabilities that may compromise the confidentiality, integrity, or availability of information assets and privacy data. The incumbent leads efforts to evaluate, mitigate, and report cybersecurity risks, ensuring compliance with state-mandated security requirements, including coordination of third-party assessments through the California Department of Technology (CDT) and the California Military Department. The role involves estimating costs of security controls, preparing confidential risk reports for management and oversight entities, and recommending risk treatment strategies. The incumbent also develops and implements incident monitoring and response policies for unauthorized access or data misuse and participates in the review of IT projects within the Project Approval Life Cycle (PAL) process. In collaboration with the State CISO and CSAC CIO, the incumbent leads security planning and contributes to the design and deployment of technical safeguards, threat countermeasures, and change management controls. The position plays a key role in

	ensuring the secure evolution of enterprise systems and services through proactive planning, security control implementation, and compliance oversight.
10% (M)	Performs other job-related duties as assigned, consistent with the classification specifications of the ITM I classification and in support of CSAC's mission and organizational initiatives. This includes contributing to special projects cross-divisionally that support vision driven goals.

IMPACT AND CONSEQUENCE OF ERROR

Significant policy misinterpretation reflects poorly on the incumbent, team members and the agency, and diminishes credibility with key stakeholders.

PROFESSIONAL CONTACTS

- Frequent contact with CSAC staff at all levels.
- Frequent contact with other state agencies and various levels of government.
- Frequent contact with the public.

OTHER SPECIAL EXPECTATIONS

- Works independently and exhibit proactive behavior with limited supervision or instruction.
- Effectively collaborates with others as a member of a team.
- Strong oral and written communication skills, particularly in the areas of presentation and facilitation.
- Strong analytical, organizational, presentation, and research skills, utilizing search engines and web/internet tools
- Positive attitude, open-mindedness, flexibility, tact, and confidentiality.
- Commitment to providing high-quality service that exceeds expectations.
- Focused attention to detail and ensures follow-through.
- Performs multiple tasks simultaneously, adhere to deadlines, and adapts to shifting priorities in a collaborative fashion.
- Effectively use professional judgment on sensitive or confidential circumstances and handles information with discretion and professionalism.
- Maintains good attendance and punctuality record.
- Consistently demonstrates a high level of initiative and sound judgment.
- Assess a situation and implements an appropriate and efficient plan of action.
- Proficient in computer technology such as Microsoft Word, Outlook, Excel, and PowerPoint, and various software programs.
- Effectively communicates information with confidence and politeness while utilizing concise and clear language within a diverse community.
- Willing to work outside regular business hours.
- Effectively utilizes division and CSAC technology and data tools with technical proficiency.

AMERICANS WITH DISABILITIES ACT (ADA) REQUIREMENT

Alternatives will be provided for those who are unable to perform the essential functions of the job due to the disability covered under the ADA.

PHYSICAL AND ENVIRONMENTAL WORKING CONDITIONS
• Exposure to computer screens and other basic office equipment. • Work in a climate-controlled office environment, open office space with artificial lighting. • Attend meetings in designated conference rooms and be willing to travel to off-site locations. • Current residency in the State of California is required. This position's location is designated in Rancho Cordova, CA and may be eligible for hybrid teleworking. The amount of telework is at the discretion of the Department and based on the CSAC's current telework policy. While CSAC supports telework, regular in-person attendance will be required at CSAC's Rancho Cordova location based on operational needs. Teleworking from outside the State of California is strictly prohibited.

EMPLOYEE ACKNOWLEDGEMENT	
I have read and understand all the requirements and information above and discussed the duties listed above with my supervisor and can perform them either with or without reasonable accommodation (RA). (If you believe you may require RA, please discuss this with your hiring supervisor. If you are unsure whether you require RA, inform the hiring supervisor who will discuss your concerns with the RA Coordinator.)	
Employee Signature	Date

SUPERVISOR ACKNOWLEDGEMENT	
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	Date

HUMAN RESOURCES OFFICE APPROVAL	
☒ Duties meet class specifications and allocation guidelines. ☐ Exceptional Allocation, form 625 on file.	
HR Analyst Initials **TA**	Date Approved **11/5/2025**

*Duties of this position are subject to change and may be revised as needed or required.