YOUR EFFORTS WILL MAKE FI$Cal A SUCCESS
DUTY STATEMENT

CLASSIFICATION TITLE Information Technology Manager II	**DIVISION NAME** Information Technology Division, Enterprise Security Services Office
WORKING TITLE Chief Information Security Officer	**POSITION NUMBER** 333-350-1406-003
EMPLOYEE NAME Vacant	**EFFECTIVE DATE** September 1, 2021

You are a valued member of the Department of FISCal. You are expected to work cooperatively with team members and others to provide the highest level of service possible. Your creativity and productivity is encouraged. Your efforts to treat others fairly, honestly and with respect are important to everyone who works with you.

GENERAL STATEMENT

Under the administrative direction of the Chief Information Officer (CIO)/ Deputy Director of the Information Technology Division (CEA B), the Information Technology Manager (ITM) II will serve as a member of Information Technology Division (ITD) senior leadership team as the Chief Information Security Officer for the Department of Financial Information System for California (FI$Cal). The ITM II serving as the information security authority in an executive management role, manages the Privacy, Information Security and Compliance program and has full responsibility for all sensitive data/systems – automated and manual, physical and logical, on-premises and cloud-deployed for the Department of FISCal. The ITM II is responsible for reviewing and implementing the activities related to the regulatory compliance and risk management that are required to protect data confidentiality and privacy rights, and for ensuring the integrity and availability of these information systems.

The ITM II has full management responsibility for organizing, planning, and directing all activities associated with the FI$Cal Enterprise Security Services Office (ESSO). As part of managing FI$Cal's Privacy, Information Security and Compliance program, the ESSO is also responsible for design, development, implementation, and ongoing support of information security tools including the Identity and Access Management (IdAM) tools and for managing the FI$Cal user access fulfillment processes. ESSO is also responsible for analyzing the FI$Cal Enterprise Resource Planning (ERP) System components and databases to identity and implement transaction and access control governance in accordance with Department of FISCal and state policies.

The duties for this position are focused in the Information Security Engineering domain, however, work may be assigned in the other domains as needed.

SUPERVISION RECEIVED
The ITM II reports directly to the CIO.

SUPERVISION EXERCISED
The ITM II manages two Information Technology Manager I staff.

The ITM II also oversees the work of consultants and partner staff who are matrixed into the ESSO.

ESSENTIAL FUNCTIONS
The incumbent must be able to perform the essential functions with or without reasonable accommodation. Specific duties include, but are not limited to, the following:

% OF TIME	ESSENTIAL FUNCTIONS
30%	**Information Security Strategic Planning and Policy Management** • Under administrative direction of the CIO, 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 FI$Cal's information security strategy and policies align with statewide information security initiatives. • Serve as the direct interface with the State Office of Information Security (OIS) on all information security policy matters; represent FI$Cal 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 FI$Cal system, data, interfaces, and the department's information processing infrastructure. • Establish cooperative relationships with management, data owners, data custodians, and information users. • Ensure that the security policies and procedures are reviewed and updated as needed to prevent new threats and vulnerabilities. The policies and procedures must address data for all media types (electronic and paper) and provide detailed processes in how to handle the data. • Research and evaluate current and new information security technology and trends to develop FI$Cal's information security strategic plan and roadmap. • Collaborate with department'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 FI$Cal security posture, utilizing inputs from staff, clients, peers and independent research in accordance with the direction of the FI$Cal CIO and the department's executive management.
20%	**Information Security Program and Risk Management** • Provide strategic direction and lead the development, implementation, and management of a comprehensive information security program to support and align the FI$Cal system and the department's information processing infrastructure with the department's mission, goals, and objectives. • Protect the FI$Cal system and the department's information and information processing assets with effective security controls. • Strategically manage the vulnerabilities, threats and incidents impacting the FI$Cal system and the department's information resources; direct the development and implementation of mitigation strategies. • Oversee the implementation of an effective information security risk management program covering risk assessment, mitigation, and evaluation. • Lead the oversight efforts for technology recovery planning and participate in the testing and documentation of issues and resolutions. • Direct security audits reviews for all major systems and data processing activities to ensure compliance with laws, statutes, regulations and FI$Cal 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 FI$Cal system and department's information resources. • Ensure staff are educated on information security and privacy protection responsibilities; ensure security training is provided to all FI$Cal staff on an annual basis.

15%	**Access Control, Governance, Risk, and Compliance** • Control and manage access, using the principle of "least privilege" to FI$Cal system and the department's IT assets to ensure that only authorized devices/persons have access as is appropriate in accordance with the business needs. • Collaborate with department's infrastructure and application development teams and ensure that security properly integrates with the system and software development lifecycle and that security requirements including the capture of adequate information for auditing are effectively addressed. • Develop enterprise-level security analytics strategy and oversee the implementation of the analytics program for transactional and access control governance. • Implement, direct and manage the data capture and analysis activities to detect potential fraud and exposure; identify solutions and coordinate their implementation to prevent fraud and exposure.
10%	**Security Infrastructure Operations** • Direct and manage the design, development, implementation, and ongoing support of information security tools including the Identity and Access Management (IdAM) solution components. • Direct and manage the design, development, implementation and ongoing support of Security Information and Event Management (SIEM) solution components. • Collaborate with the FI$Cal Infrastructure and Platform Services teams to implement and operate industry-strength tools and technologies for endpoint protection, perimeter defense, malware defense, intrusion prevention, and other preventative controls.
10%	**Administrative** • Prepare budget estimates and recommendations for procurement of services, training, and necessary information security software and services. • Proactively manage the ESSO spending and implement solutions to reduce operational costs in order to create budget for innovative applications. • Maintains currency with security technologies, policies, and standards. Attend training classes as needed. Satisfactorily complete all team-training requirements.
10%	**Staff Management** • Plan, direct, and manage the workload of ESSO staff and affiliated non-FISCal staff including consultants. • Monitor progress and performance on assignments and take appropriate action to ensure timely and successful completion

	of ESSO activities in accordance with the department and division expectations. • Lead the efforts in hiring, developing and retaining competent and professional staff that assures an adequate level of specialized analytical and technical expertise to support current and future FI$Cal needs. • Oversee development and planning for the appropriate training of staff to support emerging information technology solutions. • Motivate staff to sustain high performance. Establish and maintain proper staff recognition mechanisms. • Provide guidance and leadership to subordinate managers to develop and strengthen their leadership skills.
% OF TIME	**MARGINAL FUNCTIONS**
5%	• Perform other related duties as required to fulfill FI$Cal's mission, goals and objectives. Additional duties may include, but are not limited to, assisting where needed within the ITD, which may include special assignments.

KNOWLEDGE AND ABILITIES

All knowledge and abilities for all Information Technology classifications; and

Ability to: Manage through subordinate supervisors; effectively promote equal opportunity in employment and maintain a work environment that is free of discrimination and harassment; and effectively contribute to the department's Equal Employment Opportunity objectives.

SPECIAL REQUIREMENTS

The incumbent will use tact and interpersonal skills to develop constructive and cooperative, working relationships with others, e.g., stakeholders, customers, management, peers, etc., to facilitate communication to improve the work environment and increase productivity. **Fingerprinting and background check will be required.**

WORKING CONDITIONS

The incumbent may need to be on-site to carry out their duties. This position requires the ability to work under pressure to meet deadlines and may require excess hours to be worked. The incumbent should be available to travel as needed and is expected to perform functions and duties under the guidance of the Department of FISCal's core values. The incumbent provides back-up, as necessary, to ensure continuity of departmental activities.

This position requires prolonged sitting in an office-setting environment with the use of a telephone and personal computer. This position requires daily use of a copier, telephone, computer and general office equipment, as needed. This position may require the use of a hand-cart to transport documents and/or equipment over 20 pounds (i.e., laptop, computer, projector, reference manuals, solicitation documents, etc.). The incumbent must demonstrate a commitment to maintain a working

environment free from discrimination and sexual harassment. The incumbent must maintain regular, consistent, predictable attendance, maintain good working habits and adhere to all policies and procedures.

SIGNATURES

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 assigned HR analyst.)

_____

Employee Signature Date

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

_____

Hiring Manager Signature Date

HR Analyst PV

Date Revised: 6/26/2021