YOUR EFFORTS WILL MAKE FI$Cal A SUCCESS
DUTY STATEMENT

CLASSIFICATION TITLE Information Technology Manager I	**DIVISION NAME** Information Technology Division, Enterprise Security Services Office, Information Systems Security Management Section
WORKING TITLE Cybersecurity Manager	**POSITION NUMBER** 333-350-1405-019
EMPLOYEE NAME TBD	**EFFECTIVE DATE** TBD

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 general direction of the Chief Information Security Officer, the Information Technology Manager (ITM) I will serve as the Information Systems Security Management Section (ISSMS) Chief within the Enterprise Security Services Office (ESSO) of the Information Technology Division (ITD).

The ITM I shall have full management responsibility, including direct oversight over a team of Information Technology Specialists I/II and consultants, for organizing, planning, and directing all activities associated with this section. This ISSMS is responsible for the Financial Information System of California (FISCal)'s Program Management, Governance, Risk and Compliance, Security Engineering, and Information Asset Protection and Management.

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

SUPERVISION RECEIVED
The ITM I reports directly to the ITM II, Chief Information Security Officer.

SUPERVISION EXERCISED
The ITM I will provide direct supervision to lower level staff.

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
25%	**Program Management & Governance, Risk and Compliance (GRC)** • Develop, implement, and maintain an information security program, policies, plans, procedures and processes including defining information security roles/responsibilities. • Identify, manage, and maintain the work products required to implement the information security program and system security plans. • Perform project management functions including leading, monitoring and measuring cost, schedule and performance. • Responsible for managing risk management strategy, process and program including identify potential areas of compliance vulnerability and risk; analyze and recommend policies, guidelines, and standards; ensure an adequate system is in place to prevent, detect, and correct compliance issues. • Conduct formal risk assessments on a regular basis for all major systems and data processing activities to ensure compliance with laws, statutes, regulations and FI$Cal security policies. • Identify, review, assess, and enable business services/functions that rely on/impact information security (SaaS/PaaS/IaaS/SOCaaS services, cloud services, mobile security strategy/guidelines, new applications). • Responsible for GRC management including formulating, developing, and implementing a comprehensive, proactive, and risk-aware enterprise compliance program, including developing and implementing policies and procedures. • Responsible for Information Privacy Program including ensuring appropriate security controls based on information classification and risk to the organization to protect information privacy and ensure complaince. • Ensure that controls are adequate to meet legal, regulatory, policy, standards, privacy and security requirements (PCI, GLBA, etc.) through audits, assessments and risk analysis. • Interpret and verify adherence to specialized NIST 800 series publications to develop and conduct standardized assessment procedures to effectively protect the privacy of customer data and the security of information assets and personnel. • Coordinate with other security and privacy professionals to review policies and implement asset security controls and practices.
25%	**Systems and Application Security Engineering** • Partner with all other areas of ITD in developing and accurately maintaining security program policies, plans and procedures. • Responsible for architectural and application reviews.

	• Partner with the department's Privacy Officer to develop and enforce all applicable policies and procedures. • Responsible for coordinating, planning, developing, and maintaining data-sharing agreements with applicable partners/departments. Develop data classification framework and both maintain and protect data. • Ensure systems and applications meet applicable confidentiality, integrity, and availability requirements. • Develop and maintain a security architecture. • Address security throughout the development lifecycle and the acquisition lifecycle. • Define, implement, assess, and maintain controls necessary to protect software and applications in accordance with security requirements (operating systems, applications, database management systems, web-based PCI applications, COTS; maintenance). • Responsible for defining and maintaining identities and access controls based on identities (password management, single sign on, two factor authentication, PIN management, digital signatures, smart cards, biometrics, Active Directory, etc.). • Responsible for role-based Security Training & Awareness Program including phishing campaigns.
25%	**Asset Protection and Secure Configuration Management** • Responsible for maintaining inventories of all information assets including network (including wireless), hardware, software, system, and mobile device assets. • Responsible for maintaining defining, implementing, assessing, and maintaining controls necessary to protect networks, hardware, systems, and mobile devices in accordance with security requirements (This includes, for example, intrusion prevention and detection controls.). • Ensure secure configurations for networks, hardware, systems, and mobile devices and compliance of changes for networks, hardware, systems, and mobile device. • Responsible for maintaining defining, implementing, assessing, and maintaining controls necessary to protect information technology assets (including media) in accordance with security requirement. • Define and enforce access controls for facilities and other physical assets (such as networks and hosts).
20%	**Staff Management** • Plan, direct, motivate and manage the workload of the Information Systems Security Management section staff and affiliated non-Fi$Cal staff.

	• Monitor progress and performance on assignments and take appropriate action, including development and training, to ensure timely and successful completion of required duties in accordance with the department and division expectations. • Lead the efforts in hiring, developing and retaining competent and professional staff.
% OF TIME	**MARGINAL FUNCTIONS**
5%	• Attend training classes as needed. Satisfactorily complete all team training requirements. 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

Knowledge of: A manager's responsibility for promoting equal opportunity in hiring and employee development and promotion and maintaining a work environment which is free of discrimination and harassment; the department's Equal Employment Opportunity objectives; and a manager's role in Equal Employment Opportunity and the processes available to meet equal employment 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 environmentand increase productivity. **Fingerprinting and background check are required.**

WORKING CONDITIONS

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.

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 DG **Date Revised: 1/5/2023**