FI$Cal
One state. One system.

YOUR EFFORTS WILL MAKE FI$Cal A SUCCESS
DUTY STATEMENT

CLASSIFICATION TITLE Information Technology Specialist II	**DIVISION NAME** Information Technology Division, Enterprise Security Services Office (ESSO), Information Systems Security Management Section
WORKING TITLE Senior Security Engineer	**POSITION NUMBER** 333-350-1414-007
EMPLOYEE NAME Vacant	**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 supervision of the Information Technology Manager I, the Information Technology Specialist II (ITS II) will serve as a security engineer resource supporting the FI$Cal security architecture and enterprise working closely with Infrastructure and Platform Services teams to ensure compliance with State, Federal, and FI$Cal security requirements. The incumbent will use an advanced knowledge of network architecture to review the existing network architecture, analyze, and approve any changes to the network architecture or topography. The duties for this position are on focused in the Information Security Engineering domain, however, work may be assigned in the other domains as needed.

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.

SUPERVISION RECEIVED

The Information Technology Specialist II reports directly to the Information Technology Manager I of the Information Systems Security Management Section.

SUPERVISION EXERCISED

None

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%	**Systems and Application Security Engineering** • Lead in the development and maintenance of various information security system plans including assessing and validating applicable requirements for information technology procedures, policies, implementation, and forms. • Lead monitoring and assessing security controls within the enterprise on an ongoing basis, document changes, perform security impact analyses, and develop reports for system security statuses to the organization. • Lead analysis, design and implementation of new security technologies, architectures, and secure solutions that align with state and federal security policies and requirements. • Develop security architecture when integrating hosted services and internal solutions. • Facilitate security software/system development life cycle practices. • Review the existing network architecture, analyze, and approve any changes to the network architecture or topography by collaborating with the Enterprise Architect and the Infrastructure and Platform Services team. • Tailor configuration of the security tools deployed in all FI$Cal environments to meet enterprise security requirements and ensure effective operations of security controls that meet numerous legal and regulatory requirements. • Perform information security impact analysis techniques, procedures and reporting. • Verify new and existing solutions adhere to security requirements throughout the acquisition lifecycle. • Perform strategic planning for enterprise security architecture with various stakeholders.
30%	**Information Protection and Secure Configuration Management** • 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) • Facilitate and coordinate audits to test for the effectiveness of security controls and security architecture. • Coordinate system and software deployments and patching, enterprise solutions access activities, vulnerability scanning,

	and penetration testing, in order to ensure successful progress and execution. • Define, implement, assess, and maintain controls necessary to protect networks, hardware, systems, and mobile devices in accordance with security requirements for various security tools used for intrusion prevention and detection controls and configuration management. • Verify and recommend secure configurations for networks, hardware, systems, and mobile devices. • Verify and recommend security compliance of changes for networks, hardware, systems, and mobile device. • Verify and recommend security controls for changes and configurations of software and applications. • Apply information security assurance principles to ensure information assets are protected for confidentiality, integrity, availability, authenticity and non-repudiation of information and data. • Implement and test intrusion protection and fraud prevention and detection tools. • Create and analyze fraud data used for reporting and instruction detection. • Identify anomalous and threatening behavior and implement a viable incident response mechanism. • Analyze business impact and exposure of emerging security threats, vulnerabilities and risks and make recommends for remediating IT solutions. • Analyze and report on security technology industry and market trends as well as determine their potential impact on the enterprise.
20%	**Asset and Data Management** • Leads information technology (IT) asset management program including maintaining, monitoring and tracking IT assets to ensure accuracy, compliance and planning regarding the IT assets security posture and risk mitigation. • Categorize assets and data processed, stored, and transmitted within the assets. Manage asset hardening guidelines, implementation and testing for compliance. • Work with asset managers to ensure implementation of current guidelines. • Develop and maintain inventories of network (including wireless), hardware, system, and mobile device assets • Research, analyze and institute best practices to improve IT standards, processes, procedures, and policies for both the FI$Cal System's maintenance and operations activities.

	• Lead data management activities that involve information discovery and classification, data loss prevention and compliance. • Draft and develop queries using Structured Query Language (SQL) statements and other scripting languages to query information in FI$Cal solutions to test for security, to uncover potential issues with error handling and input validation.
15%	**Identity Management & Access Control** • Define and manage identities and access controls based on identities (password management, single sign on, two factor authentication, PIN management, digital signatures, smart cards, biometrics, Active Directory, etc.) • Define and enforce access controls for information assets including designate, prioritize, and categorize information and mission critical assets • Define and enforce access controls for facilities and other physical assets (such as networks and hosts)
<u>% OF TIME</u>	**<u>MARGINAL FUNCTIONS</u>**
5%	Perform other related duties as required to fulfill FI$Cal's mission, goals and objectives. Additional duties may include, but are not limited to, assisting where needed within the team/unit, which may include special assignments.

KNOWLEDGE AND ABILITIES

Knowledge of: Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

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 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. 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 _AR__

Date Revised: 12/27/24