CalPERS

Duty Statement

Classification: **Information Technology Manager II** **JC-400401**

Position Number: **275-817-1406-001** HCM#: **1204**

Branch/Section: **Information Security Office / Information Technology Security Services**

Location: **Sacramento, CA** Telework: Office-centered

Working Title: **Assistant Division Chief** Effective Date: **October 1, 2023**

Collective Bargaining Identifier (CBID): **M01** Supervision Exercised: ☒ **Yes** ☐ **No**

The Information Security Office (ISOF) leads the organization's effort to safeguard data, Information Technology Systems, and business processes from cyber threats. ISOF's primary responsibilities include identification, elevation and tracking of cybersecurity risks; operating several critical common controls to protect and detect potential cybersecurity incidents; establishing security standards and guidelines to meet organization and regulatory requirements; providing consultation and cybersecurity awareness training.

Under the administrative direction of the Chief Information Security Officer (CISO), the Information Technology Manager II (IT MGR II) is responsible for day-to-day operations of the information technology services and governance, risk, and compliance sections of ISOF. This role provides leadership, executive support, strategic and tactical guidance. As directed by the CISO, the IT MGR II supports and reports on strategic planning and execution of enterprise security systems, applications, and operations. As a business enabler, the IT MGR II ensures business decisions are not obstructed by cybersecurity but instead made using sound security principles and supporting CalPERS policies and plans. The IT MGR II will lead an adaptable and secure business-supporting cybersecurity team, in addition to influencing and executing with technical team members such as software developers, system engineers, cybersecurity engineers and systems administrators. The IT MGR II is expected to be skilled at effective communication and possess business acumen to align and work closely with business leaders. In addition to direct reports, the IT MGR II must be capable of working closely with C-level leadership, third parties, and audit committees. The IT MGR II must be personable and drive a synergistic team in which employees have a sustainable workload yet feel valued and challenged to achieve excellence. Recruitment, career development and retention are top personnel priorities falling under the purview of the IT MGR II. Preferably, the IT MGR II will have a technical background with the ability to comprehend technologies, their purpose, and their security requirements. The IT MGR II's technical background should encompass understanding threats, risk mitigation and technical controls.

Essential Functions

40% [1]Onsite and virtually, provide recommendations to the CISO on information security standards and best practices for Information Technology (IT) projects. Assist the CISO to oversee and manage the effectiveness of the security program. Coordinate with business partners to resolve complex or highly sensitive IT issues. Provide advice to operating units and staff at all levels on information security issues, recommended practices, and vulnerabilities. Develop and deploy the security program for assigned areas to ensure policies, procedures, and objectives are closely aligned. Assist in the development of metrics to measure the efficiency and effectiveness of the security program. Assist the CISO in strategy development and managing the information security program, focusing on security risk assessments; risk management (including risk prioritization and mitigation); education and awareness. Work with the CISO to ensure there is appropriate allocation of budgeted funds within assigned units so that the highest priority projects have sufficient monetary resources to be completed in a timely and efficient manner.

30% Onsite and virtually, ensure policy and risk controls are in place, updated when necessary, and risks are communicated to the appropriate business owners. Direct the incident response planning and management of security incidents and events to protect CalPERS assets (e.g., information, critical infrastructure, intellectual property, and reputation) in addition to investigations of security breaches and assist with disciplinary and legal matters associated with such breaches, as necessary. Provide oversight on vulnerability management, including, but not limited to maintaining a centralized scanning environment, identifying scan targets (hardware and web applications), listing and scheduling scans, and work with target owners to remediate identified vulnerabilities. Lead the disaster recovery program, including, but not limited to auditing and testing recovery plans, promoting the importance of disaster recovery and continuity planning to agencies, and the performance of business impact analyses. Interface with law enforcement agencies and other government agencies to address security lapses and responds to information security issues.

30% Onsite and virtually, respond appropriately with resources and information to requests submitted by internal and external auditing functions. Collaborate with IT Management, Legal, Compliance, Risk, Internal Audit and Human Resources in the development and implementation of policies, standards, procedures, and awareness. Maintain relationships with local, state, and federal law enforcement and other related government agencies. Maintain relationships with operating units to establish and facilitate security and risk management processes, including the reporting of remediation efforts to address negative findings; identify acceptable levels of risk; and establish roles and responsibilities concerning information classification and protection. Participate as needed in special ad-hoc committees, projects, and other IT initiatives. Perform special assignments as required. Represent CalPERS on statewide or security industry committees or task forces.

Working Conditions

- [1]This position is designated as office-centered and works primarily onsite at the Sacramento, CA Headquarters at least three weekdays.
- Workstation is located in a standard multi-level office building accessible by stairs and elevator, with artificial light, height-adjustable desk, and adjustable office chair.
- Prolonged reading and typing on a laptop or keyboard and monitor.

Conduct, Attendance and Performance Expectations

- Ability to maintain consistent attendance
- Ability to demonstrate punctuality, initiative, and dependability
- Ability to model and support CalPERS Core Values (Integrity, Accountability, Respect, Openness, Quality and Balance)
- Ability to model CalPERS Competencies and demonstrate proficiency in; Collaboration, Leading People, Leading Change, Driving Results, Business Acumen, Communication, and Leading Self.

I have read and understood the duties and essential functions of the position and can perform these duties with or without reasonable accommodation.

Employee Name (Print):

Employee Signature: ____ **Date**:

I certify that the above accurately represent the duties of the position.

Supervisor Signature: ____ **Date**: