OFFICE OF THE INSPECTOR GENERAL
Information Technology Manager I

Duty Statement

Classification Information Technology Manager I	**Working Title** Information Security Officer
Office/Unit/Section Information Technology Unit	**Team** Information Security Engineering Team
Region Headquarters	**Geographic Location** Sacramento
Position Number 297-001-1405-001	**Effective Date**
Incumbent VACANT	

SECTION A: GENERAL DESCRIPTION

Under the general direction of the Chief Information Officer (CIO), the Information Security Officer (ISO) assumes leadership of the Information Security Engineering Team. In this role, the ISO is entrusted with the responsibility of safeguarding devices, software, facilities, and infrastructure. Through close collaboration with the IT department, ISO oversee the implementation, continuous monitoring, and maintenance essential for ensuring a comprehensive cybersecurity framework. Furthermore, the ISO engages in collaborative efforts with IT and Security Operations, Security Engineering Teams, and Compliance to ensure the prompt management of patches and the reinforcement of system security. ISO also establish coordination channels with both internal and external stakeholders, including Legal, HR, and Law Enforcement, during incident response and forensic investigations. Ultimately, the ISO works collaboratively with senior management and stakeholders to align cybersecurity objectives with the overarching business goals.

SECTION B: SPECIFIC ASSIGNMENTS (w/ESSENTIAL (E) and MARGINAL (M) FUNCTIONS)

40%	(E) – Establishes, promotes, and maintains a framework for managing and communicating information security risks; develops and maintains an information security framework, including policies, procedures, standards, and guidelines; conducts regular risk assessments and develops mitigation strategies to minimize information security threats; collaborates with management, internal stakeholders and the information technology infrastructure team to ensure security requirements are integrated into business processes and systems. Responsible for the selection, deployment, and oversight of security

	tools and technologies, both on-site and remotely. Conduct assessments and manage hardware and software to safeguard systems and networks from cybersecurity threats.
35%	(E) – Oversees and leads staff responsible for: implementing and maintaining security controls, including firewalls, intrusion detection and prevention systems, encryption, and access controls; managing and securing endpoints, including desktops, mobile devices, and servers, using industry-leading tools such as MDM suites, XDR, and Antivirus; utilizes industry-standard tools to ensure prompt and efficient patch management; continuous monitoring and analysis of security logs and alerts to detect and respond to security incidents. Stay current with emerging technologies and services, both on-site and virtually, leveraging your information security expertise to develop and sustain an OIG Security Framework/Architecture.
20%	(E) – Oversees and leads information security surveys, audits, and assessments, ensuring that they remain within scope and are submitted on schedule; provides direction, evaluation, and advocacy on audit responses to minimize risks and optimize the agency's security posture; promotes compliance with applicable security regulations and standards; develops and delivers security awareness training programs to educate the organization's employees on information security best practices. Collaborate both in person and remotely with the enterprise architecture team to ensure alignment between business, technical, and security needs. Additionally, engage with IT management to synchronize the current technical infrastructure and skill sets with future architectural demands.
5%	(M) – Performs other duties as assigned, maintains on call status for after-hours and weekend support when needed.

SECTION C: SUPERVISION RECEIVED

The Information Technology Manager I is supervised by the Chief Information Officer.

SECTION D: SUPERVISION EXERCISED

The Information Technology Manager I supervises information technology staff, contract personnel, and student assistants in the Information Security domain.

SECTION E: OTHER INFORMATION

The incumbent must possess good communication skills, use good judgment in decision-making, exercise creativity and flexibility in problem identification and resolution, manage time and resources effectively, and be responsive to OIG management needs. The individual occupying this position has access to confidential or sensitive information, and is expected to maintain the privacy and confidentiality of such information at all times.

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.)

Employee Signature Date

Printed Name

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

Printed Name & Classification