Information Security Manager

About the Opportunity:

In this role, you will be responsible for planning, directing and coordinating the Agencies' information security policies and programs, setting procedures and guidelines to ensure that all information systems are functional, secure and safeguarded throughout the Agency and are in compliance with applicable privacy, customer trust and information security laws and regulations.

This position reports to the Chief Information Security Officer, and works in close day-to-day collaboration with the Chief Information Officer and the IT department.

About the Qualifications You Will Need to Join Our Team:

The ideal candidate will be a self-starter with an inquisitive, analytical mind that constantly looks for solutions to difficult problems – and who then drives for thorough, accurate and timely completion of projects. He/she will also have:

- Technical knowledge and experience: Must have deep technical knowledge and experience in security, networking, systems and database administration, architecture, or equivalent technical domain.
- Business judgement: Able to understand business requirements and develop risk management strategies that protect the confidentiality, integrity and availability of information systems and data – while maintaining alignment with business goals and operations.
- Effective communications skills: Needs to be an effective verbal and written communicator, and be able to convey complicated technology and security concepts to non-technical management and staff.

RESPONSIBILITIES AND DUTIES:

Policies and planning

- Policies: Work with the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO) to develop, enforce and maintain policies, procedures and mechanisms to protect the confidentiality, integrity, and availability of information at the Agency.
- Risk: Work with the CISO to determine acceptable risk levels for the enterprise and ensure that IT environments are adequately protected from potential risks and threats.
- Controls: Participate in development, implementation and documentation of appropriate and effective controls to mitigate identified threats and risks.
- DR/COOP: Oversee the development of information security and disaster recovery/continuity of operations programs in accordance with approved information security standards.

Ongoing security operations

- Monitoring: Conduct internal monitoring of the Agency's infrastructure (including firewalls) and serve as an internal consultant for security issues. Assist CISO in the management of any third-parties involved in security monitoring.
- IT security tools: Manage firewalls; establish settings for anti-virus/anti-malware; conduct scans.
- Access management: Monitor access to all systems and maintain access control profiles on computer network and systems. Track documentation of access authorizations to all resources.
- Incident response: With the CISO, coordinate response to detected security issues and implement solutions to reduce security risks.
- Security education and awareness: With the CISO, initiate, facilitate, and promote activities to create information security awareness throughout the Agency; administer the Security Awareness Program.
- Vendor reviews: Evaluate information security issues related to third parties in conformance with the Agency's Vendor Management policy.
- IT team member: Assist in the management of the organization's information resources in support of the goals of the Agency. Involved throughout the life cycle of information technology projects,

ensuring they are developed and deployed within the security and regulatory framework established by the Agency.

- Current IT and IT security expertise: Stay current with information security threats, practices, technologies and related regulatory issues (PCI), and deliver services that meet regulatory requirements (PCI).

Metrics and assurance

- Metrics and reporting: Work with the CISO to develop KPIs and dashboards to report and monitor security risks. Develop, document, and maintain repeatable mechanisms to determine, measure and report to management an accurate view of significant current and near-future IS-related risks.
- Testing: Perform periodic evaluations of systems and access to ensure that appropriate controls and access levels are maintained.
- Compliance: Analyze, document and track exceptions to IT policies, procedures and standards.
- Audit support: Work with internal and external auditors to document and confirm that all security administrative duties are properly performed and demonstrate overall compliance.

Other: Perform other duties and responsibilities as required or assigned by the CISO.

REQUIRED SKILLS, KNOWLEDGE AND ABILITIES:

- Strong interpersonal and leadership skills.
- Certification in IT security is required, such as CISA, CISM or CISSP.
- Bachelor’s degree in computer science or related field and a minimum of five years of progressive experience in Information Security. In-depth knowledge and experience in the following information security areas:
  - Information security assessment and auditing procedures, from both technical and business perspectives, and the use of formal methodologies
  - Vulnerability scanning and auditing tools
  - Enterprise-scale network and host-based IDS architectures
  - Enterprise-scale firewall architectures
  - Computer investigation and forensics methods and technologies
  - Secure messaging architectures
  - Privacy laws, ISO, NIST and PCI standards
- Effective verbal and written communicator.
- Successful project manager; ability to manage multiple projects and resources simultaneously.
- Experience with business continuity planning, auditing and risk management, contract/vendor negotiation and management.