INFORMATION SECURITY OFFICER

NATURE OF WORK

This is responsible professional and administrative work directing and coordinating an enterprise Information Security Program in a multi-departmental interagency environment.

Work involves translating the IT-risk requirements and constraints of the enterprise into technical control requirements and specifications; developing metrics for ongoing performance measurement and reporting; coordinating the Information Service Division's technical activities to implement and manage security infrastructure; and providing regular status and service-level reports to management. General supervision is received from the Information Services Manager with work being reviewed in the form of reports, conferences, and results achieved. Supervision may be exercised over subordinate technical and administrative personnel.

EXAMPLES OF WORK PERFORMED

Works to develop a security program and security projects that address identified risks and business security requirements.

Manages the process of gathering, analyzing and assessing the current and future threat landscape, as well as providing a realistic overview of risks and threats in the enterprise environment.

Develops budget projections based on short- and long-term goals and objectives.

Monitors and reports on compliance with security policies, as well as the enforcement of policies within the Information Services Division.

Proposes changes to existing policies and procedures to ensure operating efficiency and regulatory compliance.

Provides security communication, awareness and training for audiences, which may range from senior leaders to field staff.

Works as a liaison with vendors and the legal and purchasing departments to establish mutually acceptable contracts and service-level agreements.

Serves as an active and consistent participant in the information security governance process.

Consults with Information Services staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software.

Recommends and coordinates the implementation of technical controls to support and enforce defined security policies.

Manages security projects, such as identity and access management, network access control, and data loss prevention, and provide guidance on security matters for other IT projects.

Performs related work as required.

DESIRABLE KNOWLEDGE, ABILITIES AND SKILLS

Considerable knowledge of the principles of management and organization.

Considerable knowledge of the business impact of security tools, technologies and policies.

Considerable knowledge and understanding of information risk concepts and principles as a means of relating business needs to security controls.

Considerable knowledge of information security concepts, protocols, industry best practices and strategies.

Considerable knowledge of operating system internals and network protocols.

Considerable knowledge of the principles of cryptography and cryptanalysis.

Considerable knowledge of application technology security testing.

Considerable knowledge of system technology security testing.

Ability to interact with individuals and diverse groups, build strong relationships at all levels and across all organizations, and understand business imperatives.

Ability to manage projects including product planning, budgeting and resource allocation.

Ability to analyze security requirements and relate them to appropriate security controls.

Ability to communicate effectively both orally and in writing.

MINIMUM QUALIFICATIONS

Graduation from an accredited four-year college or university with major coursework in information security, computer science, business administration, information systems, or related field plus two years of experience in an information security role; and two years of experience in a managerial capacity; or any equivalent combination of training and experience that provides the desirable knowledge, abilities and skills.