STATE OF INDIANA CLASSIFICATION SPECIFICATION	**Class Title:** Information Security Manager		**Class Code:** 00EAO6
	FLSA Status: Exempt	**Salary Schedule:** RDS	**Effective Date:** 3-18-13
	Summary: Incumbent directs and implements the necessary controls and procedures to cost effectively protect information systems assets from intentional or inadvertent modification, disclosure, or destruction ensuring the confidentiality, integrity and availability of the information systems. Incumbent typically reports to Agency Information Technology Director or higher-level staff.		

Duties:

- Directs efforts for inclusion of information security safeguards during developmental stages of new automated and manual information systems;
- Provides guidance and direction for the physical protection of information systems assets to other function units;
- Provides reports to management regarding effectiveness of information security and makes recommendations for the adoption of new procedures;
- Determines appropriate policy and standards of information and physical security safeguards for the protection of assets and confidentiality of information, such as access authority to, or to dial into, state and visitor policy at data center;
- Directs the development, testing and implementation of information security management software programs that will monitor the integrity of sensitive application programs, computer operating systems, telecommunications network and computer hardware;
- Manages the development, implementation and testing of appropriate security plans and control techniques necessary to protect against errors and omissions, fraudulent access, espionage, sabotage, natural disaster, fire utility failures and related situations in all areas where information technology equipment, communication network and/or personnel are located;
- Conducts security lectures and training programs;
- Performs periodic audits to assure security policies and standards are being followed and recommends enhancements where necessary;
- Manages the development of procedures for detecting, reporting and investigating breaches in security, and along with Indiana State Police, directs the investigation of security breaches;
- Maintains a continuing review of existing and proposed state and federal legislation and regulatory laws pertaining to information system security and privacy and keeps management informed of changes;
- Supervises and directs the work of subordinates, including establishing and monitoring goals and objectives, training, counseling, reviewing performance;
- Performs related duties as required.

Job Requirements:

- Broad knowledge of state and federal legislation and regulatory laws pertaining to information system security and privacy;
- Broad knowledge of computer programming/languages and the operating system, mainframe/PC Local Area Network, dial-in access control techniques and on-line teleprocessing program;
- Ability to develop and maintain information security standards;
- Ability to understand and apply complex computer logic to work;
- Ability to work effectively with a wide range of information technologists, including technical support, applications development, end users and management;
- Effectively communicate both orally and in writing.

Difficulty of Work:
Incumbent applies general agency guidelines and extensive knowledge of security software, computer services operations, PC local Area Network operations, and dial-in access control techniques to develop and administer the agency's information security system. Extensive judgment and technical expertise are necessary in determining the appropriate level of security necessary so as not to interfere with service while ensuring protection of information.

Responsibility:
Incumbent serves as a technical specialist and manager of the agency's information security system and is responsible for establishing and maintaining statewide policies and safeguards to promote the security and uninterrupted operation of information technology systems and protect the privacy and confidentiality of associated databases. Incumbent must consider variables, such as personnel, communication network, physical security, data access, computer hardware and software and confidentiality in performance of work. Work is reviewed for overall attainment of goals. Errors could result in fraudulent access, sabotage and other disastrous breaches in security causing unauthorized disclosure or destruction of data.

Personal Work Relationships:
Incumbent works with departmental staff, user agencies and public officials of other local, state and federal agencies to monitor security procedures, provide guidance on information sharing and resolve problems in order to provide the desired level of security.