Detailed competency information including Competency Key Terms and Concepts, Core/Individual Attributes, Proficiency Levels, Certifications, Sample Job Titles, and Functional Perspective Statements are provided in -

APPENDIX I

State Government Information Security Competencies

1. Data (Information) Security

Refers to the application of the principles, policies and procedures necessary to ensure the confidentiality, integrity, availability and privacy of data in all forms of media (electronic and hardcopy) throughout the data life cycle.

2. Digital Forensics

Refers to the knowledge and understanding of digital investigation and analysis techniques used for acquiring, validating and analyzing electronic data to reconstruct events related to security incidents. Such activities require building a digital knowledge base. The investigative process is composed for our (4) phase: Prepare, Acquire, Analyze and Report.

3. Enterprise Architecture

Refers to the practice of applying security design principles to applications, and architecting enterprise-scale security solutions, infrastructure, processes and business activities.

4. Enterprise Continuity (Disaster Recovery)

Refers to the application of the principles, policies and procedures to ensure than an enterprise continuous to perform essential business functions after the occurrence of a wide range of potential catastrophic events.

5 Incident Management

Refers to knowledge and understanding of the process to prepare and prevent, detect, contain, eradicate and recover, and the ability to apply lessons learned from incidents impacting the mission of an organization.

6. Information Security Training and Awareness

Refers to the principles, practices and methods required to raise employee awareness about basic information security and train individuals with information security roles to increase their knowledge, skills and abilities. Training activities are designed to instruct workers about their security responsibilities and teach them about information security processes and procedures to ensure duties are performed optimally and securely within related environments. Awareness activities present essential information security concepts designed for the workforce and to affect user behavior.

7. IT Systems Operations and Maintenance

Refers to the ongoing application of principles, policies and procedures to maintain, monitor, control and protect IT infrastructure and the information residing on it during the operations phase of an IT system or application in production. Individuals with this role perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are followed as intended.

8. Network and Telecommunications Security

Refers to application of the principles, policies and procedures involved in ensuring the security of basic network and telecommunications services and data, and in maintaining the hardware layer on which it resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

9. Physical and Personnel Security

Physical Security - Refers to methods and controls used to proactively protect an organization from natural or manmade threats to physical facilities and buildings, as well as to the physical locations where IT equipment is located or work is performed (e.g., computer rooms, work locations). Physical and environmental security protects an organization's personnel, electronic equipment and data/information.

Personnel Security - Refers to methods and controls used to ensure than an organization's selection and application of human resources (both employee and contractor) are controlled to promote security. Personnel security controls are used to prevent and detect employee-caused security breaches such as theft, fraud, misuse of information and

non-compliance. These controls include organization/ functional design elements such as separation of duties, job rotation and classification.

10. Privacy

Refers to the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

State and federal law require state agencies to collect, display, retain, destroy, and dispose of records that contain personal identifying information of the residents of this state.

The collection, display, retention, destruction, and disposal of records containing the personal identifying information of state residents exposes the state and its residents to security risks, including, but not limited to, identify theft and other privacy violations.

Federal privacy law, including, but not limited to, the Privacy Act of 1974, Public Law 93-579, 5 USC 552a; the Right to Financial Privacy Act of 1978, Public Law 95-630, 12 USC 3401; and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 42 USC 1320d, impose restrictions on the collection, display, retention, destruction, and disposal by government agencies of records containing an individual's personal identifying information.

The Identity Theft Protection Act, 2004 PA 452, MCL 445.72, as amended by 2006 PA 566, requires that state departments and agencies that own or license personal information included in a database or that maintain a database of personal information notify residents of this state of the unauthorized access and acquisition of that information if the department or agency determines that the security breach is likely to cause substantial loss or injury, or result in identity theft to that resident.

State government is firmly committed to ensuring not only that government is accountable for the personal information and personal identifying information of state residents for which it is responsible, but that the residents of the state understand the manner in which their personal identifying information is collected, displayed, retained, destroyed, and disposed of by state government and understand their rights when that information is used or accessed without authorization.

11. Policies, Standards and Compliance (Information Assurance)

Refers to the application of the principles, policies and procedures that enable an enterprise to meet applicable information security laws, standards and policies to satisfy statutory requirements, perform industry-wide best practices and achieve information security program goals.

Information Assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability and non-repudiation.

12. Procurement

Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements (SLA), justifications required by policies or procedures, and contract administration plans.

13. Security Risk Management

Refers to the policies, processes, procedures and technologies used by an organization to create a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment and to manage mitigation strategies that achieve the security needed at an affordable cost.

14. Strategic Security Management

Refers to the principles, practices, and methods involved in making managerial decisions and actions that determine the long-term performance of an organization. Strategic security management requires the practice of external business analyses such as customer

analyses, competitor analyses, market analyses, and industry environmental analyses. It also requires the performance of internal business analyses that address financial performance, performance measurement, quality assurance, risk management, and organizational capabilities/constraints.

The goal of these analyses is to ensure that an organization's IT security principles, practices, and system design are in line with its mission statement.

15. Systems and Application Security

Refers to the principles, policies and procedures pertaining to integrating information security into an IT system or application during the SDLC prior to the Operations and Maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the enterprise and its information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation and software security standards compliance.

3.0 INFORMATION SECURITY ROLES, COMPETENCIES AND FUNCTIONAL PERSPECTIVES

Eight roles have been identified to segment the many job titles within the state government information security workforce into manageable functional groups. Each of these roles represents a cluster of organizational positions/job titles that perform similar functions in the workplace with the appropriate information security competencies.

3.1 CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer (CISO) specializes in the information and physical security strategy within an organization supporting the strategic use and management of information, information systems and information technology. The CISO is charged with the development and subsequent enforcement of the organization's security policies and procedures, security awareness and education programs, business continuity and disaster recovery plans, and all security-related regulatory compliance issues.

Competencies:

- **Data (Information) Security**: *Manage, Evaluate*
- **Digital Forensics**: *Manage, Evaluate*
- **Enterprise Architecture**: *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Manage*
- **Incident Management**: *Manage*
- **Information Security Training and Awareness**: *Manage*
- **IT Systems Operations and Maintenance**: *N/A*
- **Network and Telecommunications Security**: *Evaluate*
- **Physical and Personnel Security**: *Manage*
- **Policies, Standards and Compliance (Information Assurance:)** *Manage, Evaluate*
- **Privacy**: *Manage, Design, Evaluate*
- **Procurement**: *Manage, Design, Evaluate*
- **Security Risk Management**: *Manage, Design, Implement, Evaluate*
- **Strategic Security Management**: *Manage, Design, Implement, Evaluate*
- **System and Application Security**: *Manage, Evaluate*

Example Job Titles :

- **Chief Information Security Officer (CISO)**
- **Executive Director, Information Security**
- **Director, Information Security**

3.2 PRIVACY OFFICER

The Privacy Officer is responsible for developing and managing an organization's privacy compliance program. Privacy implementation is the application of the principles, policies and procedures, and compliance to laws, regulation, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. The Privacy Officer establishes a risk management framework and governance model to assure the appropriate handling of Personally Identifiable Information (PII) and ensures that PII is managed throughout the information life cycle from collection to disposal. Included is integration of the appropriate privacy security controls and technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

Competencies:

- **Data (Information) Security**: *Manage, Design, Evaluate*
- **Digital Forensics**: *Evaluate*
- **Enterprise Architecture**: *N/A*
- **Enterprise Continuity (Disaster Recovery)**: *Evaluate*
- **Incident Management**: *Manage, Design, Implement, Evaluate*
- **Information Security Training and Awareness**: *Design, Evaluate*
- **IT Systems Operations and Maintenance**: *N/A*
- **Network and Telecommunications Security**: *N/A*
- **Physical and Personnel Security**: *Design, Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Design, Implement, Evaluate*
- **Privacy**: *Manage, Design, Implement, Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Manage, Design, Implement, Evaluate*
- **Strategic Security Management**: *N/A*
- **System and Application Security**: *Evaluate*

Example Job Titles :

- **Chief Privacy Officer (CPO)**
- **Privacy Officer (PO)**
- **Privacy Specialist**

3.3 INFORMATION SECURITY OFFICER OR MANAGER

The Information Security Officer (ISO) or Information Security Manager (ISM) specializes in the information and physical security strategy within an organization. The ISO or ISM is charged with the development and subsequent enforcement of the organization's policies and procedures, security awareness program, business continuity and disaster recovery plans, and all industry and governmental compliance issues. The ISO or ISM reports to the Agency Director (Secretary, Commissioner, etc.). The ISO or ISM:

- Manages an agency's information security program by overseeing and ensuring agency compliance with policies and procedures regarding the security of information assets.
- Must be of a sufficiently high-level job classification and/or position/job description that can execute the responsibilities of the office in an effective and independent manner.
- Establishes security policies and procedures.
- Understand the business process needs.
- Assesses internal and external risks and the respective business impact.
- Provide appropriate mitigation strategies.
- Stay current on state statutes, state/federal laws and regulations.
- Provide oversight responsibility at the agency level for ensuring the integrity and security of automated files, databases, and computer systems.
- Provides approval of proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data
- Determine aforementioned proposals meet all provisions of agency information security and risk management policies

- Approves the use of alternatives to support encryption for the protection of confidential, personal and sensitive information stored on portable electronic storage media and portable computing devices
- Approves any business use of peer-to-peer technologies

Competencies:

- **Data (Information) Security**: *Manage, Design, Evaluate*
- **Digital Forensics**: *Implement*
- **Enterprise Architecture**: *N/A*
- **Enterprise Continuity (Disaster Recovery)**: *Evaluate*
- **Incident Management**: *Design, Implement, Evaluate*
- **Information Security Training and Awareness**: *Design, Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *N/A*
- **Network and Telecommunications Security**: *N/A*
- **Physical and Personnel Security**: *Manage, Design, Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Manage, Design, Implement, Evaluate*
- **Privacy**: *Implement*
- **Procurement**: *N/A*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Evaluate*

Example Job Titles :

- **Information Security Officer**
- **Information Security Manager**
- **Information Security Agency Lead**

3.4 COMPLIANCE OFFICER (INFORMATION ASSURANCE)

The Compliance Officer is responsible for overseeing, evaluating and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Compliance Office provides guidance and autonomous evaluation of the organization to management.

Information Assurance practitioners ensure, verify and validate the protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and protection against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Competencies:

- **Data (Information) Security**: *Evaluate*
- **Digital Forensics**: *Evaluate*
- **Enterprise Architecture**: *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Evaluate*
- **Incident Management**: *Evaluate*
- **IT Security Training and Awareness**: *Design, Evaluate*
- **IT Systems Operations and Maintenance**: *Evaluate*
- **Network and Telecommunications Security**: *Evaluate*
- **Physical and Personnel Security**: *Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Manage, Design, Implement, Evaluate*
- **Privacy**: *Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Implement, Evaluate*
- **Strategic Security Management**: *Evaluate*
- **System and Application Security**: *Evaluate*

Example Job Titles :

- **Compliance Officer**
- **Inspector General**
- **Certification and Accreditation Engineer**
- **Information Assurance Engineer**
- **Analyst**
- **Specialist**
- **Risk Assurance Specialist**
- **Software Quality Assurance Analyst**
- **Computer Systems Validation Engineer**
- **Cyber Security Analyst**
- **Project Director**
- **Project Manager**

3.5 INFORMATION SECURITY ENGINEER

The Information Security Engineer applies cross-disciplinary IT and information security knowledge to build technology systems that remain dependable in the process of conducting business and in the face of malice, error and mischance.

Competencies:

- **Data (Information) Security**: *Design, Implement, Evaluate*
- **Digital Forensics**: *Design, Evaluate*
- **Enterprise Architecture**: *Manage, Design, Implement*, *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement, Evaluate*
- **Incident Management**: *Design, Implement, Evaluate*
- **IT Security Training and Awareness**: *Design, Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Design, Implement, Evaluate*
- **Network and Telecommunications Security**: *Manage, Design, Implement*, *Evaluate*
- **Physical and Personnel Security**: *Implement, Evaluate*

- **Policies, Standards and Compliance (Information Assurance)**: *Implement*
- **Privacy**: *Design, Evaluate*
- **Procurement**: *Design, Evaluate*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **Information Security Engineer**
- **Information Security Architect**
- **Systems Engineer**
- **Technology (Data) Center Operations Engineer or Manager**
- **Operations Manager**
- **Systems Analyst**
- **Digital Forensics Manager**
- **Risk, Security and Facilities Specialist**
- **Information Technology Infrastructure Analyst**
- **Systems Analyst**
- **Information Security Analyst**
- **Requirements Analyst**
- **Software Architect**

3.6 INFORMATION SECURITY PROFESSIONAL

The Information Security Professional concentrates on protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.

The Information Security Professional also includes the Information Security Procurement Professional. The Information Security Procurement Professional is responsible for purchasing and negotiating for products (e.g., software and hardware) and services (e.g., contractor support) in support of an organization's IT strategy. In the information security context, they must ensure that security requirements are specified within solicitation and

contract documents (Sarbanes-Oxley, FISMA, etc.) and that only products and services meeting requirements are procured. Information Security Procurement Professionals must be knowledgeable about their industry and their own organization, and must be able to effectively communicate with supplies and negotiate terms of service.

Competencies:

- **Data (Information) Security**: *Design, Implement*
- **Digital Forensics**: *Implement, Evaluate*
- **Enterprise Architecture**: *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement, Evaluate*
- **Incident Management**: *Design, Implement,, Evaluate*
- **IT Security Training and Awareness**: *Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Evaluate*
- **Network and Telecommunications Security**: *Evaluate*
- **Physical and Personnel Security**: *Design, Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance)**: *Implement, Evaluate*
- **Privacy**: *Design, Implement, Evaluate*
- **Procurement**: *Design, Implement, Evaluate*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement, Evaluate*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **Information Security Professional**
- **Information Technology Security Analyst**
- **IT Security Analyst**
- **Systems Analyst**
- **IT Security Technical Analyst**
- **Research Specialist**
- **Digital Forensics Analyst**

- **Purchasing Manager**
- **Acquisition Manager**
- **Buyer**
- **Contracting Officer**
- **Contract Specialist**
- **Purchasing Specialist**
- **Facility Security Officer**
- **Physical Security Administrator**
- **Personnel Security Officer**

3.7 INFORMATION SECURITY OPERATIONS & MAINTENANCE PROFESSIONAL

The IT Security Operations and Maintenance Professional ensures the security of information and information systems during the operations and maintenance phases of the software development lifecycle (SDLC).

Competencies:

- **Data (Information) Security**: *Implement, Evaluate*
- **Digital Forensics**: *Implement*
- **Enterprise Architecture**: *Implement*, *Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement*
- **Incident Management**: *Design, Implement, Evaluate*
- **IT Security Training and Awareness**: *Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Manage, Design, Implement, Evaluate*
- **Network and Telecommunications Security**: *Manage, Design, Implement, Evaluate*
- **Physical and Personnel Security**: *Evaluate*
- **Policies, Standards and Compliance (Information Assurance)**: *Implement, Evaluate*
- **Privacy**: *Implement, Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Implement*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **IT Security Engineer**
- **Operations and Maintenance Engineer**
- **Operations and Maintenance Manager or Supervisor**
- **Information Technology Specialist**
- **Database Administrator**
- **Directory Services Administrator**
- **Network Administrator**
- **Service (Help) Desk Representative**
- **Technical Support Personnel**

3.8 INFORMATION SECURITY SYSTEM ADMINISTRATION PROFESSIONAL

The Information Security System Administration Professional supports the application of the principles, policies and procedures, and compliance with laws, regulations, statutes, etc. used to ensure the confidentially, integrity, and security of individual personal information. Includes the integration of privacy and the appropriate security controls into information technologies that support secure internet-based business systems and transactions, and converting existing business processes to web-enabled e-business processes (online transactions, business to consumers (citizen) and business-to-business).

Competencies:

- **Data (Information) Security**: *Design, Implement, Evaluate*
- **Digital Forensics**: *Implement*
- **Enterprise Architecture**: *Implement, Evaluate*
- **Enterprise Continuity (Disaster Recovery)**: *Design, Implement, Evaluate*
- **Incident Management**: *Design, Implement, Evaluate*
- **IT Security Training and Awareness**: *Implement, Evaluate*
- **IT Systems Operations and Maintenance**: *Manage, Design, Implement, Evaluate*

- **Network and Telecommunications Security**: *Manage, Design, Implement, Evaluate*
- **Physical and Personnel Security**: *Design, Implement, Evaluate*
- **Policies, Standards and Compliance (Information Assurance):** *Implement, Evaluate*
- **Privacy**: *Evaluate*
- **Procurement**: *Evaluate*
- **Security Risk Management**: *Design, Implement, Evaluate*
- **Strategic Security Management**: *Implement*
- **System and Application Security**: *Design, Implement, Evaluate*

Example Job Titles :

- **System Administrator**
- **Database Administrator**

4.0 STATE GOVERNMENT INFORMATION SECURITY COMPETENCY & FUNCTIONAL MATRIX

Work conducted by the information security workforce is complex and not all work in a given competency area is performed by a single role. Work performed by a team of individuals with different responsibilities and spans of control ranges from creating the strategy for a component of the Information Security Program, to development of the program's scope and procedures, to performing hands-on implementation work, and to evaluating the work's efficiency and effectiveness. Rather than all roles being responsible and knowledgeable in all areas of information security and having the ability to perform all job tasks, individual roles are associated with a subset of competencies to represent the work performed as part of an Information Security team. The type of work performed is resolved by role through the four (4) functional perspectives (Manage, Design, Implement, and Evaluate) across a series of technical competency areas. It is on these functional perspectives that an individual should be evaluated if a role-based certification truly measures his or her ability to perform.

To present a visual depiction of the relationship among state government information security roles, competencies and functional perspectives that describe work performed in that role, the *State Government Information Security Competency & Functional Matrix* is provided on the following page.

Information security roles are broadly grouped into Executive (Managerial), and Functional (Technical) categories. When a role is mapped to a competency, and to a functional perspective within that competency, it defines *all* of the functions the role performs within the functional perspective.

> Example:
>
> An Information Security Officer who develops procedures related to "Incident Management" is mapped to the "Design", "Implement", and "Evaluate" functional perspectives within the "Incident Management" competency area and would perform work within these functional perspectives.

STATE GOVERNMENT INFORMATION SECURITY *Competency & Functional Framework*			STATE GOVERNMENT INFORMATION SECURITY ROLES													
			Executive (Managerial)								*Functional (Technical)*					
Functional Perspectives: M - Manage; D - Design; I - Implement; E - Evaluate			Chief Information Security Officer		Privacy Officer		Information Security Officer or Manager		Compliance Officer (Information Assurance)		Information Security Engineer		Information Security Professional		Information Security Operations & Maintenance Professional		Information Security System Administration Professional	
INFORMATION SECURITY COMPETENCIES	1	Data (Information) Security	M		M	D	M	D				D		D				D
				E		E		E		E	I	E	I		I	E	I	E
	2	Digital Forensics	M									D						
				E		E	I			E		E	I	E	I		I	
	3	Enterprise Architecture									M	D						
				E						E	I	E		E	I	E	I	E
	4	Enterprise Continuity (Disaster Recovery)	M									D		D		D		D
						E		E		E	I	E	I	E	I		I	E
	5	Incident Management	M		M	D		D				D		D		D		D
					I	E	I	E		E	I	E	I	E	I	E	I	E
	6		M			D		D		D		D						

	Information Security Training and Awareness				E	I	E		E	I	E	I	E	I	E	I	E
7	IT Systems Operations and Maintenance										D			M	D	M	D
									E	I	E		E	I	E	I	E
8	Network and Telecommunications Security									M	D			M	D	M	D
			E						E	I	E		E	I	E	I	E
9	Physical and Personnel Security	M			D	M	D						D				D
				I	E		E		E	I	E	I	E		E	I	E
10	Policies, Standards and Compliance (Information Assurance)	M			D	M	D	M	D								
			E	I	E	I	E	I	E	I		I	E	I	E	I	E
11	Privacy	M	D	M	D						D		D				
			E	I	E	I			E		E	I	E	I	E		E
12	Procurement	M	D								D		D				
			E		E				E		E	I	E		E		E
13	Security Risk Management	M	D	M	D		D				D		D				D
		I	E	I	E	I	E	I	E	I	E	I	E	I		I	E
14	Strategic Security Management	M	D														
		I	E			I			E	I		I	E	I		I	
15	System and Application Security	M									D		D		D		D
			E		E		E		E	I	E	I	E	I	E	I	E

Figure 4-1 State Government Information Security Competency and Functional Matrix

5.0 STATE GOVERNMENT INFORMATION SECURITY JOB/POSITION DESCRIPTIONS

The following sample information security job/position descriptions from the six (6) pilot states are provided. Additional examples will be added as other states contribute to the model framework.

- Chief Information Security Officer (CISO)
- Director, Division Information Security
- Privacy Officer
- Information Security Officer (ISO)
  - Also Included:
    - "*Implementing an Effective State Government Information Security Program*" - Explains ISO/ISM roles and responsibilities.
    - Information Security Officer (ISO) Survey
- Information Security Manager (ISM)
- Technology Center Operations – Systems Analyst – Risk, Security & Facilities Specialist
- Information Technology Security Analyst – Information Security Policy Analyst
- Information Security Analyst – Enterprise Information Security Analyst
- Research Specialist
- Systems Analyst – Information Security Technical Analyst
- Information Security Administration
  - Information Technology Specialist I
  - Information Technology Specialist II
  - Information Technology Specialist III