Information Security Guide for State of Georgia Government Executives

May 2008

Georgia Technology Authority
Office of Information Security
47 Trinity Avenue, S.W.
Atlanta, Georgia 30334

Purpose

Governor Perdue is moving Georgia forward to becoming the best managed state in the country. How we manage technology and use it to improve customer service is part of that plan. In March 2008, the Governor emphasized this point by issuing an executive order creating agency-level information security reports.

State of Georgia senior executives are charged with many responsibilities, including appropriately protecting state and federal information. It is important that as a senior executive, you receive information explaining those information risk management responsibilities as well as identifying the resources you may use to discharge those responsibilities. This guide's purpose is to inform you of those responsibilities and to aid you in their execution.

This document is a starting point. Much of the information used by state agencies is unique to a particular agency. This guide is targeted as an introduction to this topic and is not intended to be a comprehensive instruction manual on information risk management.

The Georgia Technology Authority (GTA) wishes to acknowledge the National Institute for Standards and Technology (NIST) publication, NISTIR 7359, and the NIST website as the source for much of the information contained in this document. GTA choose to model Georgia's information risk management program after the federal program developed by NIST and overseen by the President's Office of Management and Budget. As you read this document, you will gain an understanding of the benefits provided by this model.

Introduction

The commissioner or head of each agency within Georgia's state government is responsible for developing and implementing an information security program for their agency. This responsibility may be delegated within their organization, but the commissioner retains overall responsibility for the program. This guide is intended as a starting point for those commissioners and their delegates charged with creating and managing each agency's information security program.

Information security is more properly termed information risk management. It is the business processes associated with determining how to appropriately minimize, transfer or assume the risks associated with information assets (computers, data, etc.). An information security program focuses on three attributes of information: its confidentiality, integrity, and availability (CIA). For purposes of information security, these three terms are defined as follows (44 U.S.C 3542):

> "... confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; ..." A loss of confidentiality is the unauthorized disclosure of information.
>
> "... integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; ..." A loss of integrity is the unauthorized modification or destruction of information.
>
> "... availability, which means ensuring timely and reliable access to and use of information." A loss of availability is the disruption of access to or use of information or an information system.

Not all information requires the same level of controls (methods of protection), and sometimes it is possible for different information or systems to share controls. Treating information security as a risk management program allows management to use appropriate controls while controlling the associated expenses. Senior management is responsible for:

- establishing the agency information security program
- setting program goals and priorities that align with and support the mission of the agency
- measuring the effectiveness of the overall program, and
- ensuring resources are available to support the success of the information security program.

Most executives understand the importance of a strong information security program. Their questions are usually focused on what they need to do to be successful. As with any successful program, information security starts with senior leadership's commitment to the program.

Senior leadership must focus on effective information security governance and support, which requires integration of security policies, standards, and guidelines into the strategic and daily

operations of an agency. There are several key security questions that emerge for the executive.

- Why do I need to invest in information security?
- Where do I need to focus my attention in accomplishing critical information security goals?
- What are the key activities to build an effective information security program?
- What are the information security laws, regulations, standards, and guidance that I need to understand to build an effective information security program?
- Where can I learn more to assist me in evaluating the effectiveness of my information security program?

This document provides answers to these questions.

Why do I need to invest in information security?

State agencies gather, process, use, and dispose of information in the course of delivering vital functions to the citizens of Georgia. Much of that information has security requirements documented in laws, regulations, policies and standards. State executives are charged with creating information security programs that ensure compliance with those requirements.

More specifically, much of the information used by state agencies is owned by the federal government. The federal government requires that such information be protected in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the Office of Management and Budget Circular No. A-130, Appendix III.

The benefits of compliance are many. For example,

- Mission success and resilience – The information exists to support the agency with its mission. If it is not available or is corrupted, the mission may be put at risk.

- Increased public confidence – Proactively addressing risks increases confidence in state government and the agency.

- Executives may be held accountable – State executives may face administrative and/or legal action for non-performance of their assigned responsibilities. In addition, their agency may be fined or denied the use of federally controlled information for non-performance. This could potentially impact an agency's ability to deliver on its core mission. Information security is ultimately the responsibility of the agency head and those officials assigned to information security roles.

- Risk management matures over time and integrates with agency operations – As the information security program matures, the risks associated with information become more understood and better managed. The risk reduction methodologies will become integrated with business processes associated with information technology, avoiding the issues rather than fixing them at a later date.

- More effective financial management – Solving issues early in any process avoids unnecessary corrective action later in the process, making the process more efficient. This leads to more effective financial management of information assets.

Appropriate investment in information security allows executives to manage information security risks as a core component of their overall governance practice. It is merely part of their overall risk management program.

Since so many state systems must be managed under the FISMA Risk Management Framework, GTA has selected this framework for use with all state systems. This alignment was selected to eliminate conflicting requirements and to further control the costs associated with information security.

Where do I need to focus my attention in accomplishing critical information security goals?

The key focus areas required to develop a strong information risk management program are similar to any other successful program. Namely:

- Strong leadership is the foundation of any successful program, and an information security program is no different. It requires an executive commitment to the program, and it requires the setting expectations for improved security performance.

- Information security program development requires time and a comprehensive approach. Executives must understand that information security should integrate with all facets of an agency's operations. Developing an information security program will require time for it to mature. The amount of time will depend on many factors, some of which will be unique to each agency. It is important to develop metrics for measuring progress and continuing to improve the overall program.

- Be proactive vs. reactive. Sound business practices require developing the ability to anticipate issues so they may be resolved proactively. Information security is no different. By integrating information security into all agency business processes, subject matter experts will develop the ability to avoid pitfalls before they occur.

- People can make or break your program. There are no silver bullet technology solutions for information security. At its core, every high-functioning information security program is based on the concept of people anticipating and either avoid or reduce risks, and having the appropriate staff to address incidents when they occur. The information security program requires appropriate staffing and training.

What are the key activities to build an effective information security program?

The National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC) has developed a suite of documents on this topic, many as part of the FISMA implementation project. Some are regulatory law (federal information processing standards or FIPS) while others are collaboratively produced documents on key information security topics (called special publications or SP). Georgia is leveraging this work for use within state agencies.

The NIST documents are flexible enough to allow effective use at the federal level by agencies of all sizes and with differing missions, goals and objectives. Each Georgia agency will need to tailor their activities in a similar manner. However, there are some required activities in common for all successful information security programs. They are:

- establishing effective governance structure and agency-specific policy
- demonstrating management support to information security
- integrating information security elements into a comprehensive information security program, and
- measuring and reporting the effectiveness of the security controls.

The 12 required elements are listed below. At the end of each section the applicable NIST and GTA documents are listed. These documents are available for free on the NIST website, http://csrc.nist.gov, or from GTA's website, http://gta.georgia.gov.

1. Security Planning

Security planning begins at the enterprise or organizational level and filters all the way down to the system level. It is imperative to create an organizational infrastructure that supports security planning while positioning the appropriate staff into key roles.

- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, Chapter 8 Security Planning
- FIPS PUB 199, *Standards for Security Categorizations of Federal Information and Information Systems*
- FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*

2. Capital Planning

Increased competition for limited budgets and resources requires that agencies allocate available funding toward their highest priority information security investments. The recommended method of prioritization is to categorize all information systems according to their impact levels (see NIST publication FIPS-199) and to prioritize those with higher impact levels.

Another consideration is the appropriateness of the risks. If the system with higher impact levels has been assessed through the risk management program and has an acceptable amount of residual risks, it may be appropriate to prioritize the lower system.

- NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*

3. Awareness and Training

The security awareness and training program is a critical component of the information security program. People are at the core of information security, and these programs will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information resources entrusted to them.

- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*

4. Information Security Governance

The purpose of information security governance is to ensure that agencies are actively implementing appropriate information security controls to support their mission in a cost-effective manner. It influences information security policy development, oversight, and ongoing monitoring activities. Continuous monitoring of the information threat landscape and making adjustments over time are key functions of information security governance.

- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, Chapter 2 Governance

5. System Development Life Cycle

The system development life cycle (SDLC, which usually stands for software development life cycle) is the overall process of developing, implementing, and retiring information systems. Various SDLC methodologies have been developed to guide the processes involved, and some methods work better than others for specific types of projects. Typically the following phases are addressed: initiation, acquisition, development, implementation, maintenance, and disposal. Information security is a key component of any SDLC.

- NIST SP 800-64 Rev. 1, *Security Considerations in the Information System Development Life Cycle*

6. Security Products and Services Acquisition

Information security services and products are essential elements of an organization's information security program. Agencies should use risk management processes when selecting security products and services as a method of determining their actual value to the agency.

- NIST SP 800-35, *Guide to Information Technology Security Services*

- NIST SP 800-36, *Guide to Selecting Information Technology Security Products*

7. Risk Management

The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Risk management can be viewed as an aggregation of three processes that have their roots in several federal laws, regulations, and guidelines. The three processes are risk assessment, risk mitigation, and evaluation and assessment.

Georgia models its risk management program after the risk management framework created by NIST in support of the Federal Information Security Management Act (FISMA) of 2002. This framework is required for all information systems that contain federally controlled information, and it is also the new audit standard for the Georgia Department of Audits. This is discussed more in the section on laws and regulations.

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

8. Certification, Accreditation, and Security Assessments

Security certification and accreditation (C&A) are important future activities that will support a risk management process, and each is an integral part of an agency's information security program. The C&A process is designed to ensure that an information system will operate under appropriate management review. Security controls are the management, operational, and technical safeguards prescribed for an information system to protect the system and its information.

- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*

9. Configuration Management

Configuration management (CM) ensures consideration of potential security impacts due to specific changes to an information system. It reduces the risk that any changes made to a system may result in a compromise. Organization must ensure that management is aware of, has reviewed and approved proposed changes.

- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*

10. Incident Response

A well-defined incident response capability helps an organization to detect incidents quickly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly.

- NIST SP 800-61, *Computer Security Incident Handling Guide*

11. Contingency Planning

IT contingency planning is one element of a larger contingency and continuity of operations planning program that encompasses IT, business processes, risk management, financial management, crisis communications, safety and security of personnel and property, and continuity of government.

- NIST SP 800-34, *Contingency Planning for IT Systems*

12. Performance Measures

Governor Perdue has ordered GTA to collaborate with the Georgia Department of Audits and Accounts and with the Governor's Office of Management and Budget to establish standards for agency information security reports. Each fall, GTA will compile these reports to create the state's Enterprise Information Security Report. This report will aid state decision makers in their consideration of information security matters.

Performance measures are a key feedback mechanism for an effective information security program. Agencies can develop information security metrics that measure the effectiveness of their security program and provide data to be analyzed.

- NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*
- NIST Draft SP 800-80, *Guide for Developing Performance Metrics for Information Security*
- GTA Information Security Standard for Agency, *Information Security Reporting*

What are the information security laws, regulations, standards, and guidance that I need to understand to build an effective information security program?

1. FISMA has been interpreted to apply to any system operated by or on behalf of the state that uses federal information or that tracks the use of federal funds. The law requires federal agency that are information owner (i.e. Health and Human Services owns medical records) to ensure that its information is properly protected regardless of its location.

   Federal agencies are contacting Georgia agencies to obtain FISMA required documentation and to assess the compliance of state information systems. To satisfy FISMA, state agency systems must be fully FISMA compliant as defined by NIST and the Federal Office of Management and Budget (OMB). This requirement applies to many of the major information systems operated by the state.

2. Governor Perdue's executive order, *Regarding information security reporting*, requires state agencies to report annually about their information security program. The required format and content for those reports is specified in GTA's Information Security Standard for, Information Security Reporting, available on GTA's website. Those reports are due to GTA by the end of July, and they will be compiled into an, *Enterprise Information Security Report,* to be published each October.

3. GTA is authorized by law to "establish technology security standards and services to be used by all agencies[1]." Official Code of Georgia Annotated (O.C.G.A.) § 50-25-4(a)(21) (2006).

   GTA revised its information security policies and standards to align them with the FISMA implementation project run by NIST. It is GTA's objective to use FISMA as a model for all information security practices within the state to avoid both conflicting requirements and duplication of effort. It is also believed this will lead to economies for the state as a whole.

4. The Georgia Department of Audits and Accounts (DOAA) has developed a new information security assessment methodology based on NIST Draft SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. It is expected that this methodology will be used for all state systems.

[1] Agency is defined as "every state department, agency, board, bureau, commission, and authority which shall not include any agency within the judicial branch of state government or the University System of Georgia and shall also not include any authority statutorily required to effectuate the provisions of Part 4 of Article 9 of Title 11." O.C.G.A. § 50-25-1(b)(1) (2006).

Where can I learn more to assist me in evaluating the effectiveness of my information security program?

When a Georgia executive is responsible for a program, it is important for the program to have metrics for evaluating the effectiveness of the program. Information security is no different. Each information security program should compile metrics at two levels, per information system and per agency. As stated above, there are two NIST documents for developing information security related metrics.

A could method for evaluating an information security program is to compare it to other programs within the state. Starting in 2008, GTA will collect individual reports from all state agencies and compile them into an Enterprise Information Security Report. Each agency may compare themselves with their peers by examining that report.

There are two statewide organizations where agency executives may learn more about information security. They are the CIO Council and the ISO Council. These bodies meet monthly, and the ISO Council is dedicated to information security related topics.

GTA's Office of Information Security is also available as a resource to state executives. The Office of Information Security staff may be contacted directly by email at gta-ois@gta.ga.gov. GTA has also published information security related information on its website, http://gta.georgia.gov.

A final method would be to examine federal resources. These include:

- NIST (http://www.nist.gov)
- NIST's Computer Security Division (http://csrc.nist.gov)
- The Office of Management and Budget (http://www.whitehouse.gov/omb)
- The Federal CIO Council (http://www.cio.gov)

Conclusion

Executive leadership is the key for any successful information security program. A successful program will require funding, staffing and oversight. By placing an appropriate emphasis within the agency on information security, executives will set in motion the activities necessary to create and sustain a robust information security program.

It is also important to keep information security in perspective as a form of risk management. As with other forms of risk management, information security should be part of the agency's governance model, and it should be fully integrated with agency operations. Planning for information security considerations during the business cycle will reduce development and implementation times and will involve key stakeholders at all levels of the organization.

A successful information security program places the agency's executive team in a proactive position related to information risk management. The program produces executive level information and metrics, allowing decision makers to base information risk management decisions on reliable information.