

**2009 NASCIO Recognition Award Nomination
State of Georgia**

Nomination Category:
Information Security and Privacy

Title of Nomination:
Georgia Enterprise Information Security Report

Nomination Submitted By:
Patrick Moore
Chief Information Officer
Executive Director
Georgia Technology Authority

Executive Summary

As recently as late 2007, the state of Georgia had no means of documenting or evaluating state agencies' information security programs or compliance with policies and standards across the state's IT enterprise. The state was at risk, leading Governor Sonny Perdue to comment, "I cannot even assure Georgians that we have the basic, essential security and disaster recovery levels worthy of a 24-hour-a-day, seven-day-a-week operation serving the needs of over nine million Georgians."

During the preceding three years, the state had issued more than four million notification letters to citizens whose private information had been exposed from state computers. Most of the state's high-impact systems—those in which a security incident could potentially result in catastrophic financial damage to the state and/or physical harm to a person—had never undergone a security assessment.

In response, the Georgia Technology Authority worked with the Governor's Office on an [Executive Order](#) requiring state agencies to report each year on the status of their information security programs, and the state adopted the Federal Information Security Management Act (FISMA) of 2002's [Risk Management Framework](#) for all state information systems. Signed by Governor Perdue in March 2008, the order led to the publication in October 2008 of the state's first [Enterprise Information Security Report](#), which incorporated data from 109 state agencies.

The report showed that agencies in all three branches of state government are making information security a priority. For the first time, 48 of the state's 64 complex agencies (those with more than just an informational website and e-mail) submitted a complete security inventory of their information systems. Sixteen of those 48 agencies rated at least one of their information systems as high-impact. Just under a third of high-impact information systems have security plans that comply with the state's new requirements. In addition, the report showed that 92 percent of employees in the agencies with high-impact systems received security training.

To ensure ongoing improvement, the report included Plans of Action and Milestones, which establish clearly defined goals for state agencies in 13 different security-related areas.

The report is already yielding valuable results, which will be compounded as agencies build on their progress from year to year. It provides state leadership with appropriate information in a consistent format to support their fact-based decision making. Uniform reporting standards also help to ensure that the state's information security controls are consistent across the enterprise. The standards allow for differing requirements of state agencies and their federal partners and enable the state to identify risks and set priorities for corrective actions without exposing vulnerabilities to inappropriate parties.

Description of the Business Problem and Solution

"I cannot even assure Georgians that we have the basic, essential security and disaster recovery levels worthy of a 24-hour-a-day, seven-day-a-week operation serving the needs of over nine million Georgians."

*--Georgia Governor Sonny Perdue,
December 2007*

The concerns Governor Perdue voiced in late 2007 were supported by facts pointing to the state's inadequacies in information security:

- Over the previous three years the state had issued more than four million notification letters to citizens whose private information had been exposed from state computers.
- GTA's firewall systems were blocking between 5,000 and 35,000 inappropriate connection attempts every minute.
- The state had 88 separate agency-level information security programs; less than a third of them were able to produce a list of the information systems within their programs.
- Over 70 percent of the state's high-impact systems had never undergone a security assessment.

The state had no means of documenting or evaluating state agencies' information security programs or compliance with policies and standards across the state's IT enterprise. State agencies used a variety of reporting standards, making it difficult to measure information security across state government or to track progress from year to year.

In response, the Georgia Technology Authority worked with the Governor's Office on an [Executive Order](#) requiring state agencies to report each year on the status of their information security programs, and the state adopted the [FISMA risk management framework](#) for all state information systems. Signed by Governor Perdue in March 2008, the order led to the publication in October 2008 of the state's first [Enterprise Information Security Report](#), which incorporated data from 109 state agencies. The content of the report was specified by GTA in coordination with the State Accounting Office and the Governor's Office of Planning and Budget. Its focus areas included information security awareness, the implementation of the FISMA risk management framework, business continuity planning, and incident response planning.

The report closely followed the adoption of the new statewide information security program in early 2008. The program provides the first comprehensive framework for managing and reporting on the information risks associated with operating the state's

infrastructure. Among the program's major components are 67 newly adopted information security policies and standards based on FISMA.

Significance of the Project

Since Governor Perdue took office in 2003, he has remained committed to improving IT operations as part of his goal of making Georgia the best managed state in the nation. Governor Perdue has a deep appreciation of the importance of a well-managed information technology enterprise in achieving his vision for Georgia. "Technology is the underpinning of a well-run, modern-day enterprise," he said. "It is the cornerstone of making decisions that will lead our state to being the best-managed state."

Georgia's Enterprise Information Security Report is yielding valuable results, which will be compounded as agencies build on their progress from year to year:

- State leaders have the information they need to oversee the security of the state's IT resources.
- A single comprehensive framework ensures that the state's information security controls are effective across the enterprise.
- The reporting standards allow for differing requirements of state agencies and their federal partners.
- The reporting standards enable the state to identify risks and set priorities for corrective actions without exposing vulnerabilities to inappropriate parties.
- The state is better able to control associated expenses by utilizing agency-level risk management practices.

Ultimately, the most important beneficiaries of the report and the information security improvements it fosters are the citizens of Georgia. They will be better able to trust that their private information entrusted to the state is secure at all times.

With security ranked as number 4 among NASCIO's State CIO Priorities for 2009, many states may be interested in developing consistent reporting standards as Georgia has. The Enterprise Information Security Report could be easily adopted.

Benefit of the Project

The first Enterprise Information Security Report was published in October 2008 and incorporated data from 109 of the state's 113 agencies. (Three other agencies submitted statements about their need to remain separate; all have mature security programs with public reports.) For the first time, state leaders have information about each agency's level of compliance with the state's information security standards. This information is useful when they make funding decisions.

The report found that state agencies are making significant progress in complying with a comprehensive set of [Information Security Policies, Standards and Guidelines](#).

Summary of findings

The enterprise report showed that agencies in all three branches of state government are making information security a priority.

- 48 of the state's 64 complex agencies (those with more than just an informational website and e-mail) submitted a complete security inventory of their information systems.
- 16 of those 48 agencies rated at least one of their information systems as high-impact, which means a security incident could potentially result in catastrophic financial damage to the state and/or physical harm to a person.
- 29 percent of high-impact information systems have security plans complying with the state's new requirements.

State agencies are also training employees to understand their role in information security. Because awareness training is considered the most cost-effective way to improve information security, GTA produced a [security awareness video](#) to assist agencies in educating staff.

- Although training materials were not available until April 2008, agencies reported training 50 percent of their employees by the end of FY 2008. The state employs approximately 88,000 workers.
- 92 percent of employees in the 16 agencies with high-impact systems received security awareness training.

The report included [Plans of Action and Milestones](#), which establish clearly defined goals for state agencies in 13 different security-related areas:

1. Non-responsive Agency

All 113 organizations will either report or decline to participate by the report due-date for FY 2009.

2. Formalize Participation by Outsourcing Agencies

All outsourcing agencies should have formal agreements for this arrangement or be operating their own security program by June 30, 2009.

3. Classify Agencies by Impact Categorizations

Agencies should be classified according to the highest impact rating of the systems operated by the agency by March 31, 2009.

4. Security Awareness Training

Ninety-five percent of all state workers will receive security awareness training by June 30, 2009.

5. System Inventories

All complex agencies will provide or update their inventories, including impact categorizations, during FY 2009.

6. System Security Plans

Seventy-five percent of all high-impact systems and 25 percent of all moderate-impact systems will have approved security plans by June 30, 2009.

7. Desktop Security

One hundred percent of all security plans will expressly address workstation security issues by June 30, 2009.

8. System Security Assessments

Seventy-five percent of all high-impact systems will undergo independent third-party assessments during FY 2009.

9. Disaster Planning

One hundred percent of all systems with an availability impact rating of high will have availability or disaster recovery plans that support those requirements by June 30, 2009.

10. Business Continuity Planning Participation

One hundred percent of the agency security activity participation agreements should explicitly state whether it includes BCP functions by June 30, 2009.

11. Business Continuity Planning

One hundred percent of the agencies will have a minimal BCP by June 30, 2009.

12. Incident Response Planning

All agencies with high-impact or moderate-impact information must have approved security incident management and response plans approved by GTA by June 30, 2009.

13. Strategy

GTA will evaluate the state's existing security strategy and make adjustments where necessary, including extending it to include four years, by December 31, 2008.

Progress on the Plans of Action will be measured in future reports. The reporting standard for the 2009 agency information security reports was issued on March 31, with agency submissions due July 31. The 2009 Enterprise Information Security Report will be published in October of this year.