

| | | |
|---|--|---------------------------------|
|  Georgia Technology Authority | Georgia Technology Authority | |
| Title: | Information Technology Reporting | |
| PSG Number: | SS-08-053.04 | Topical Area: Technology |
| Document Type: | Standard | Pages: 3 |
| Issue Date: | 3/31/11 | Effective Date: 3/31/11 |
| POC for Changes: | GTA - Enterprise Governance and Planning Division | |
| Synopsis: | Requires agencies to report the status of their information technology projects and security program to GTA. | |

PURPOSE:

On March 19, 2008 the Governor issued an Executive Order taking the lead on issues of information security. This order directs GTA to define performance measures and issue a standard in March of each year requiring agencies to report the status of those measures as of the end of the fiscal year to GTA. This is consistent with GTA's role established in legislation; "To establish technology security standards and services to be used by all agencies;" (see O.C.G.A 50-25-4(a)(21). In 2009, new legislation updated GTA powers to ". . . publish an annual state information technology report;" and the authority to solicit reporting data from agencies up to twice a year (see O.C.G.A 50-25-7.10).

GTA will compile and analyze the agency reports to assess the adequacy and effectiveness of information security and IT processes throughout the state and recommend areas for improvement. GTA will prepare and submit an annual State of Georgia Information Technology Report to the Governor's Office. The annual report will provide a high-level view of the state's information technology assets and projects and their criticality to the state. The report will facilitate state executives' and legislators' understanding of the current state of information technology, security and related risks and how each agency is performing in meeting the needs of its organization and managing those risks year to year. It will also provide data needed for prioritizing and making cost effective, risk-based decisions with regards to recommended improvements.

In 2011, GTA will continue obtaining and maintaining ongoing information regarding each agency's information security program, technology assets, projects and expenditures.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

- Official Code of Georgia Annotated:
 - O.C.G.A 50-25-4(a)(21)
 - O.C.G.A 50-25-7.10

| | |
|--------|----------------------------------|
| Title: | Information Technology Reporting |
|--------|----------------------------------|

- Governor's Executive Order on Information Security Reporting 19 March 2008
- Enterprise Information Security Charter (PS-08-005.01)

SUPPLEMENTAL EXCEPTION:

While information security plans and measures are specifically exempted from public disclosure under the Open Records Act, agencies are required to strategically plan their IT initiatives and make these plans and corresponding performance measures or metrics available to the public.

Any exceptions to this standard shall be at the discretion of and approved in writing by the State Chief Information Officer.

STANDARD

To ensure the adequacy, effectiveness, and continuous improvement of information assurance throughout the state:

1. GTA shall define the performance goals and measures as follows:
 - a. IT performance goals and measures shall be based on specific compliance, implementation and effectiveness objectives such as but not limited to compliance with technology and security policies and standards, cost-effective service delivery, project management and mission accomplishment.
 - b. The performance goals shall state a desired result of the implementation of system security and IT process requirements and the actions required to accomplish the goals.
 - c. The metrics shall attempt to measure the accomplishments of each agency by quantifying the level of implementation, effectiveness and efficiency of the stated objectives.
 - d. The metrics, over time, shall demonstrate progress against established objectives as technology services and security matures and shall facilitate the development of corrective actions and/or improvement plans.
2. Each agency shall conduct an annual review and report the status of its operational IT systems, applications, IT projects and information security program as of June 30th of each year.
3. Agencies shall deliver their completed report to GTA, utilizing the web-based Information Technology Governance Reporting (ITGR) system, not later than July 31st of the same year.
 - a. No other format for the report will be accepted.
 - b. The web address for the ITGR system will be sent to agency heads and CIOs.
4. GTA shall compile and analyze the agencies' reports and produce an annual State of Georgia Information Technology Report and deliver to the Governor's office by October 1st of each year

| | | |
|-----------------|----------------|--------|
| Effective Date: | March 31, 2011 | 2 of 3 |
|-----------------|----------------|--------|

| | |
|--------|----------------------------------|
| Title: | Information Technology Reporting |
|--------|----------------------------------|

- a. The report shall provide a summary of statewide IT resources, projects and expenses as well as performance strengths, weaknesses and areas of improvement.
- b. It shall include recommendations to improve the maturity of IT processes, governance and security throughout Georgia government.

In addition to continuous update of each agency's IT system, application and project inventories, 2011 performance measures shall seek demonstrated progress over 2010 each agency's technology operations and project management and information security processes in the areas of:

- o Security Program Management
- o Business Continuity and Disaster Recovery Planning
- o Incident Response and Reporting
- o Security Education and Awareness
- o Enterprise Performance Lifecycle Management (EPLC)

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- GTA's full collection of information security and technology policies and standards are available on its website; <http://gta.georgia.gov>

REFERENCES

- NIST Computer Security Resource Center- <http://csrc.nist.gov/>
 - o SP 800-53 rev 3 Information Security Controls:
 - PM-1,2
 - PM-4,5,6
 - o SP 800-55 Performance Measurement Guide for Information Security
 - o SP 800-80 Guide for Developing Performance Metrics for Information Security

TERMS and DEFINITIONS

- **Performance Goal** – The desired results of implementing the security objective or technique that are measured by the metric
- **Performance Measures** – The actions required to accomplish the performance goal validated through the completion and analysis of the agency report.
- **Metric** – Numeric indicators used to gauge state-wide program performance and monitor progress toward accomplishing state-wide goals and objectives. Monitors and measures accomplishment of goals by quantifying the level of implementation and effectiveness

| | | |
|-----------------|----------------|--------|
| Effective Date: | March 31, 2011 | 3 of 3 |
|-----------------|----------------|--------|