

# 2009 Agency Information Security Report (AISR) Frequently Asked Questions (FAQ)

## General Information, Process and System Access

Q1: Does my agency have to report and why do we have to do it every year?

A: Governor Perdue's executive order (EO) requires annual reporting by all Executive Branch agencies. All other agencies are required (based on AG interpretation of GA code) to adhere security standards published by GTA and are strongly encouraged to follow the executive order.

Each year state leaders must make important decisions regarding strategic goals and objectives for the coming year. The annual security report is a tool to help facilitate informed decision making in support of those goals. It provides a uniform method to regularly measure the health of the enterprise on information security and risk management matters that affect how the state manages the enterprise, the services it provides and the information entrusted to its care.

The report also demonstrates quantifiable progress in accomplishing strategic goals by identifying areas that require more focus and highlighting those areas where the enterprise exemplifies being the best managed state, providing the citizens of Georgia with visibility into the health of the state's enterprise and confidence in its ability to service them and protect their information.

Q2: What were the findings from last years reporting? Was a final report published?

A: GTA consolidated and analyzed the data from each AISR and in October 2008, presented to the Governor, the legislature and agency heads; the Enterprise Information Security Report. The report provided a complete analysis of the findings and a Plan of Actions and Milestones for this year. The final report and other supporting information are publicly available on GTA's public website at:  
[http://gta.georgia.gov/00/channel\\_title/0,2094,1070969\\_84340779,00.html](http://gta.georgia.gov/00/channel_title/0,2094,1070969_84340779,00.html)

Q3: What is the deadline for submitting my agency's AISR?

A: AISR timeline and deliverables (all dates are for year 2009):

March 31	GTA publishes the AISR Standard for that year
NLT June 15	GTA makes AISR website available to agencies to complete their AISR online. This new AISR website will become available year round for agencies to update their information as necessary rather than waiting for June of each year.
July 31	Completed and Approved AISRs due to GTA
Oct 31	GTA publishes annual State of Georgia Enterprise Information Security Report

Q4: What time period does the report cover?

A: As per Governor's Executive Order, each agency shall report on the status of their agency's information security program as of June 30<sup>th</sup> of each year. This means that the report should pertain to the current fiscal year. For example, in 2009, the reporting period will cover FY 2009 (July 1, 2008 to June 30, 2009).

Q5: What is the consequence to my agency if we aren't able to show progress on the 2008 Plan of Actions and Milestones?

A: The EISR is intended to measure information security maturity from the perspective of the Enterprise. While it is understandable that some agencies are further along on the maturity scale than others, the EISR is NOT intended to "punish" agencies who still have work to do in these areas. Instead it is intended to be a tool to highlight areas for improvement and facilitate management decisions that will help the agency continue to progress up the maturity scale.

Q6: When will the AISR website be available and how do I get access?

A: The new AISR website is schedule to go live June 1, 2009. Its commencement and web address will be communicated to all agency heads, CIO's, and ISO's.

In order to gain access, agency personnel must register online on the AISR website (address and link to be announced at commencement). The AISR administrator will verify the user and enable the user to access user's agency report. The registration and verification results will be communicated to the user via email messages normally within 24 hours.

Q7: Can I register for an AISR website account on behalf of my commissioner or others in my agency that need access?

A: Yes. Go through the online registration process as you would for yourself, but enter the person's data for whom the user account is being created. The AISR administrator will validate the user data and notify the user via email when their account is created.

Q8: Do I have to use the AISR Website to do my reporting?

A: Yes. Unlike last year, all reports must be submitted through the new AISR website created for this purpose. No other forms will be acceptable.

Q9: Who in my agency is required to complete this report?

A: Per the Governor's executive order, the Executive Director of the agency is responsible to report the status of their agency's information security program. He/She may delegate the task of completing the report to one or more personnel within that agency.

The AISR website accommodates multiple users from an agency to register and access their agency's report. Each user may complete different sections of the report based on their function within the agency. This decision is left to the agency. Among the users registered on the AISR website for your agency, one user must be designated as "Agency Head" during registration process. GTA prefers this user be the Executive Director. However, the Executive Director of the agency may nominate another user to act on his/her behalf. This nomination must be communicated to GTA in writing. Please see Q&A below explaining the process.

The "Agency Head" user on the AISR website will have the additional ability to "Finalize and Approve" the report upon its completion. After the agency's report is marked as "Finalized and Approved" by the "Agency Head" user, the report will be locked and available in READ-ONLY mode and no updates can be performed.

Q10: My agency's Executive Director wants me to sign off as the "Agency Head" for the completed AISR. Can I do that?

A: Yes. When you register on the AISR website, mark the check box for "Agency Head" in the user profile page. However, your agency executive director or commissioner must formally delegate this designation to you using the template letter below and provide the letter to GTA. The AISR administrator will verify that the letter was received before granting you this access.

<p>----- PLEASE USE OFFICIAL AGENCY STATIONERY  FAX THIS LETTER TO 404-478-9421 -----</p> <p>DATE:</p> <p>To: Mark Reardon Chief Information Security Officer Georgia Technology Authority 47 Trinity Ave. Atlanta, GA 30334</p> <p>Ref: Delegation of authority to finalize and approve &lt;Agency Name&gt; Information Security Report</p> <p>Dear Mr. Reardon: I, &lt;Name of Agency Commissioner&gt;, the commissioner (or exec dir whichever applies) of &lt;AGENCY NAME&gt; delegate the following person to finalize and approve our Agency Information Security Report for 2009.</p> <p>Name: Title:</p>
--

Regards,  
name and signature of commissioner

Q11: In last year's report my agency was qualified as a "small" agency and we did not have to complete the full AISR. Why do we have to complete the full report this year?

A: Every agency imposes a certain level of risk to the enterprise and the constituency regardless of its size. After conducting the analysis of last year's data, it was determined that it is more relevant to group agencies by their potential impact to the enterprise which is determined by their collective systems' high water mark (highest impact categorization).

Q12: Our agency provided a lot of this information last year. Can I access last year's system data or do I have to re-enter it again?

A: While it is our intention to minimize the level of effort required to complete the 2009 AISR, were unable to find an efficient way to extrapolate and import 2008 system dataset into the new AISR system and meet the new reporting style and requirements. We apologize for this inconvenience but assure you that all data entered from this year forward will be continually available for review and maintenance.

However, the information provided by your agency for 2008 report is available in the "Enterprise Information Security Report for FY 2008" accessible at [http://gta.georgia.gov/00/channel\\_title/0,2094,1070969\\_84340779,00.html](http://gta.georgia.gov/00/channel_title/0,2094,1070969_84340779,00.html)

Appendix-E and Appendix-F of the "Enterprise Information Security Report for FY 2008" contains the entire dataset supplied by your agency.

Q13: We're a GAIT agency, isn't GTA (its vendors) responsible for the risk and security management of our systems?

A: NO. Under GAIT, GTA manages the IT service provider/s ONLY. The service provider operates and maintains the technology as directed by the system owners. Each agency affected by GAIT (or any agency using a service provider) always retains ownership of its business and is always responsible for ensuring adequate protection of the data used to support that business. Therefore, Business Owner's must define the operational and security requirements for its data and ensure those requirements are being met. The service provider is responsible for meeting those requirements as requested, directed and paid for by the customer in the most efficient manner possible.

Q14: I have finished my AISR but I cannot select the "Finalize and Approve" option in the AISR website, why not?

A: Only a user designated as the "Agency Head" has permissions to approve and lock the finished AISR. By default, your commissioner (or Executive Director) has this designation. However, he/she may delegate this designation to you by providing GTA

with the letter described in Q9. If this letter has been sent to GTA, contact the AISR Administrator (see Q17).

Q15: My agency head or designee has locked/finalized our agency's AISR but we need to make some changes. Can we have it unlocked?

A: Yes. Contact the AISR Administrator (see Q17) for assistance.

Q16: Our agency will not be able to complete the AISR by the July 31<sup>st</sup> deadline. Can we request an extension?

A: Extension requests are not recommended but are sometimes unavoidable and will be handled on a case-by-case basis. All extension requests must be approved by the State CIO Patrick Moore. Contact the AISR Administrator (see Q17) for more information.

Q17: Who do I contact if I have other questions or need help with the AISR website?

A: Please direct all AISR system and security related questions to the AISR Administrator, Tometrice Strickland at email [gta-eis@gta.ga.gov](mailto:gta-eis@gta.ga.gov) or phone 404-463-8474.

Q18: Who do I contact if I have questions or need help with expenditure information?

A: Direct IT Expenditures questions to: Woody Dover at email [woody.dover@gta.ga.gov](mailto:woody.dover@gta.ga.gov) or phone 404-657-7166

AISR Standard - Appendices 1-2  
Security Program Management

Q18: We're a GAIT agency, isn't GTA (its vendors) responsible for the risk and security management of our systems?

A: See Q13

Q19: In last year's report my agency was qualified as a "small" agency and we did not have to complete the full AISR. Why do we have to complete the full report this year?

A: See Q11

Q20: How do I know if another agency has risk and security management responsibility for my agency?

A: Consider the following scenarios:

- Your SAISO (Information Security Officer) is assigned to another agency
- Your agency does not own the IT systems or business applications that support your agency
- Your agency uses another agency for email services, office automation services and/or you are only a user of another agency's business applications

If your answers to any of the above scenarios is affirmative, then it is very likely that your agency is "matrixed" (from an IT perspective) to another agency.

However, these scenarios do not in anyway confirm your status and you must have a signed agreement with that agency.

Q21: Our agency has other agencies "matrixed" to us for IT. What do we do from a security reporting perspective?

A: You may report on behalf of that agency. However, you must have a signed agreement with that agency indicating that they are covered by your information security program. You must include their employee headcount with your agency's employee headcount and include them when responding to all applicable reporting areas within the report.

Q22: Is there a template or an example letter for the "outsourced" security and risk management program agreement?

A: No. Last year, GTA reached out to agencies that we believed might be in this situation. This year, the responsibility lies with the affected agencies to formalize an agreement between themselves. The agreement or understanding should detail the IT

security and risk management responsibilities and denote who will be reporting for whom.

Q23: What is a SAISO?

A: Senior Agency Information Security Officer, formerly referred to as Agency ISO. This is the formal title (under NIST) of the primary/lead/senior person in each agency managing the information security program for that agency.

Q24: Why are you asking about a Privacy Officer? Is it required?

A: A Privacy Officer is not required. However, with the every increasing legislation and legal issues regarding privacy matters (both personal and professional), industry is recognizing the need to rely on individuals with specialized expertise in the area of privacy to focus in these matters. This question identifies those agencies that have chosen to create this function.

AI SR Standard - Appendix 3  
Security Awareness and Training

Q25: Is there a new/updated security awareness video or can we reuse the security awareness video from GTA from last year?

A: Reuse of the security awareness video from last year is appropriate to meet the general user annual requirement and/or you may use other material as your agency sees appropriate.

Q26: How can I access GTA's security awareness video?

A: Please contact Walter Tong via email: [walter.tong@ga.gov](mailto:walter.tong@ga.gov) or phone: 404-651-9754.

AISR Standard - Appendix 4  
Security Risk and IT Portfolio  
Management

Q27: Our agency provided a lot of this system information last year. Do we have to re-enter it again?

A: See Q12

Q28: Why do I have to document the characteristics of all my systems?

A: To effectively run and improve a business, the business must understand the risks. To understand the risks and effectively mitigate them (security), the business must know what it has, how it uses it and what it needs. To know this and make crucial business decisions systems must be fully and accurately documented.

Q29: What is a "system" versus an "application"?

A: NIST defines a "system" as a discrete set of information resources (workstations, servers, applications, network, etc) working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. For the purposes of the AISR we are loosely defining a system as all of the above minus the business applications that support your agency's mission. Operational systems are those IT systems that are readily available, in use and actively supporting the business. Operational systems do not include research, development or test systems. It is also common in the industry nomenclature to call these systems "Production Systems".

Q30: How does a Business Owner "knowingly" accept risk?

A: The Business Owner is ultimately responsible for ensuring appropriate confidentiality, integrity, and availability of information. He/she must be fully aware of the risks associated with operating an information system or application that supports his/her business area and has taken the necessary steps to either mitigate those risks or accept them.

Q31: There are 8 phases to the Risk Management Framework but only phases 1-6 are discussed. What about phases 7 and 8?

A: The 8 phases of the framework are sequential and continuous and performing them all as intended assumes a level of information assurance maturity and that security is integral to the lifecycle of an information system. Based on the findings from the 2008 EISR, the enterprise still has work to do to accomplish the first phase, which is to appropriately categorize its data. Phases 2-5 require that security controls be identified, refined, implemented and documented. While most of the enterprise systems are currently operational and controls are in place, our findings from the 2008 EISR showed that most agencies are not fully aware of the controls that are in place, have not

documented those controls for which they are aware in a security plan nor assessed the effectiveness of those controls either through a self-assessment or through an independent third-party as required in phase 6. Therefore, phases 7 and 8, at this stage in the enterprise maturity, are irrelevant.

Q32: Does an audit by the State Department of Audits and Accounts (DOAA) qualify as an internal assessment or an independent 3<sup>rd</sup> party assessment?

A: Yes and No. While DOAA is considered an independent 3<sup>rd</sup> party for some types of audits, they do not currently perform FISMA-based security assessments. Therefore, for the purposes of this report and adherence to the Independent Security Assessment standard, audits performed by DOAA, DO NOT qualify.

Q33: Do we have to reports assessments conducted for all systems? Last year we were only required to report assessments for systems categorized as High.

A: Yes. We are now collecting the same information for all systems regardless of their impact rating. This allows us to analyze and report the data in multiple ways based on the objectives for that year. However, the standard that addresses assessments still applies to systems categorized as HIGH.

Q34: We do an IT Expenditures Report every September. Why is the IT Expenditures information being asked for in the Information Security Report?

A: There are several reasons including but not limited to the following:

1. There are several synergies and inter-dependencies between the various data i.e. "reports" that are requested and gathered from the agencies. Significant efficiencies could be obtained in the use and analysis of this data if it were gathered and stored in a more integrated manner. GTA is attempting to maximize these efficiencies by streamlining how and what information is requested from agencies and reducing the number of separate but interrelated inquiries to agencies. Providing this information with the AISR will mean that agencies will not be asked to complete an IT Expenditures Report in September.
2. Information security risk management is integral to IT risk management which is integral to overall business risk management. Effective management of IT related risk includes understanding the costs associated with planning for and operating an information system or application that supports business objectives.
3. The ultimate goal of all reporting activities is to help achieve one of the Governor's strategic goals of becoming the best managed state. Taking a holistic, enterprise view of the state's IT environment enables state leaders and state agencies to work together to better manage the risks enterprise-wide and make informed fiscal decisions regarding the systems that provide the services of the state.

Q35: How are agency SAISOs or other IT professionals supposed to know the answers to these IT expenditure questions?

A: Although we have consolidated the reporting mechanisms, the required reporting information will not likely come from a single source within the agency. The AISR website supports multiple users with an agency. Please direct the various sections of

the report to the appropriate business units or personnel within your agency. Whomever from your agency completed the IT Expenditures Report in past years will likely be the source to complete it this year. The only difference is the delivery format and reporting tool.

Q36: Explain what is meant by expenditures for infrastructure?

A: Infrastructure expenditures are the costs incurred during the current reporting year for all of the physical hardware (servers, desktops, laptops, PDAs etc), software, networks, facilities (data centers), etc., that are required to develop, test, deliver, monitor, control or support IT Services. Infrastructure also includes but is not limited to transmission media; such as telephone lines, cable television lines, satellites and antennas. It includes the firewalls, routers, aggregators, repeaters, and other devices that control transmission paths as well as the software used to send, receive, and manage the signals that are transmitted, operating systems and office automation applications. Infrastructure for the purposes of the AISR, does not include the business applications, associated personnel (FTE salaries), processes, or documentation.

If available, provide information based on subclass in which the expenditure actually occurred.

Q37: Explain what is meant by expenditures for operating an application?

A: Application costs are all costs incurred during the current reporting year for the business applications including special line item grants, service/maintenance contracts, service calls, equipment, training, documentation, processes etc. DO NOT include costs for personnel (FTE salaries) or costs for network/communications infrastructure or other hardware not specifically designated for this application.

If available, provide information based on subclass in which the expenditure actually occurred.

Q38: What is the Program or subprogram name (Prioritized Program Based Budget)

A: For budgeting purposes an agency is divided into "programs" based on its strategic goals and objectives. If necessary these programs are subdivided based on more specific strategic goals and objectives into "subprograms". These program and subprograms have associated budgets. For Example: Department of Natural Resources (DNR) is divided into the following programs: Administration, Coastal Resources, Parks, Historic Preservation, Environmental Protection, Pollution Prevention Assistance, and Wildlife Resources. These programs may have subprograms with specific budgets.

Business applications support 1 or more programs and/or subprograms within an agency. For each application, provide the name/s of the program/s and/or subprogram/s that are supported by this application.

Q39: As a GAIT agency, we get a bill from GTA for the services provided. How do we differentiate our infrastructure vs. application expenditures?

A: Under GAIT, in scope agencies obtain itemized billing for infrastructure, network and applicable support expenditures.

Q40: Explain what is meant by expenditures for a project?

A: A Project is defined as those IT related aspects of a business goal that will cost more than \$100,000. Project expenditures are all costs incurred during the current reporting year including FTE salaries. A subset of costs incurred for some projects are from non-state issued sources. Finally, there is a lifecycle for all projects that should have estimated costs projected for its analysis, development, implementation, operations, maintenance and eventual decommissioning including FTE salaries.

Q41: Does FTE (full-time equivalent) include contractors/consultants?

A: Yes, EXCEPT where "agency" or "contractor" FTE information is specifically requested.

Q42: How do I calculate full-time equivalents (FTE) if I have consultants, part-time staff or staff splitting their time supporting multiple systems or applications?

A: Calculate FTE for salaried positions:

- A full-time budgeted position = 1.0
- If 10% of a staff position is spent supporting this application the FTE would be:  $1.0 \times .10 = .10$
- If 5 staff positions each spend 10% supporting this application the FTE would be:  $5 \times .10 = .50$

Calculate FTE for hourly positions (also use for hourly contractors/consultants)

- Total annual hours of time spent supporting this application divided by 2,080 (52 weeks/yr x 40 hrs/week = 2,080 hours annually = full-time)
- If full-time hourly position spends 988 hours supporting this application during the year, the FTE calculation is:  $988 \text{ divided by } 2080 = .48$  (rounded)
- If part-time hourly position works 500 hours annually and spends 10% of that supporting this application, the FTE calculation is:  $500 \times .10 \text{ divided by } 2080 = .02$  (rounded)

Q43: What is meant by FTEs for infrastructure support and applications support?

A: Infrastructure FTEs are full-time budgeted positions such as system/network administrators, help desk, web masters, communications techs and other technicians that support the operating infrastructure.

Application FTEs are full-time budgeted positions such as sys admins, application developers/testers/trainers, database admins, user/floor help and people who support application processes like QA, operators etc.

Q44: How do I provide the "general age" of my IT assets?

A: On the AISR website, we have reworded the question and associated table to read: Provide the quantity of all your assets by type/platform and provide the number of those assets that are GREATER than >5 years old and the depreciated value of those aged assets. "Age" in the table has been replaced with " Number > 5 years old" and Depreciated Value added "(of assets > 5 years)".

Q45: Under GAIT, GTA has collected a lot of the requested information related to IT projects, IT assets etc. Will GTA answer these questions?

A: NO, GTA will not answer these questions on your behalf. However, if you believe that GTA (or anyone for that matter) has the information you need to complete your report, please do not hesitate to contact the SMO for GAIT agencies (or whomever) to obtain the information you need.

Q46: Will data reported in the AISR (e.g. system and application names) be made public?

A: Yes. Any information reported in the AISR is subject to the Open Records Act. It is widely accepted within the industry that system/application names are NOT considered "sensitive". However, the name in conjunction with IP addresses, network diagrams, system security plans or assessment findings ARE sensitive and will NOT be made public via the EISR. If you feel that the name of your systems or applications is sensitive please use a "covert" name that is still identifiable to your agency head, CIO and the Governor's Office.

AISR Standard - Appendix 5  
Business Continuity Planning

Q45: What is an ESF? How do I know if my agency is an ESF?

A: ESF stands for Emergency Support Function. ESF agencies are identified in the Governor's executive order (EO) and the Georgia Emergency Operations Plan (GEOP) as having primary and/or support responsibilities to provide essential services or support for those services during a man-made, natural, or environmental state emergency. Go to [www.gema.gov](http://www.gema.gov) to review the EO and the GEOP to find out if your agency is listed as an ESF.

Q46: Our Agency has a Disaster Recovery Plan (DRP) why isn't that sufficient for a Business Continuity Plan (BCP)?

A: Business Continuity describes how an organization prepares for, responds to and recovers critical business functions before, during and after a significant business disruption. The goal is for critical business processes to be sustained while the supporting infrastructure (facilities, technology, people) is recovered. DR addresses only the recovery of the technology that supports business. BCP involves several interdependent components, each with its own focus and objective but together create the Business Continuity Plan. Below is a table of the "pieces" to BCP:

BCP	Business Sustainment	Contingency Planning	Disaster Recovery	Business Resumption/Recovery
Focus and Objectives	Identify and Sustain Critical Business Processes	- Establish Critical Business Process Workarounds - Make Do	Identify, Prioritize and Restore IT Operations	- Post Emergency - Complete Business Restoration (including support functions) - Return to Business as usual.

Q47: Who do I call if I need help with BC Planning and/or the BCP Tool provided by GTA?

A: Contact Jack Welch **E-Mail:** [jack.welch@ga.gov](mailto:jack.welch@ga.gov) **Office:** 404.463.5907

AISR Standard - Appendix 6  
Security Incident Response and  
Reporting

Q48: How do I submit my agency Security Incident Management Plan to GTA?

A: Submit your completed plan via email to: [gta-eis@gta.ga.gov](mailto:gta-eis@gta.ga.gov) All plans will be reviewed and approved by GTA/EGAP and GBI. A copy will be retained on file with GTA/EGAP.

Q49: How can I find out if my agency Security Incident Management Plan has been approved?

A: Contact Walter Tong, Dir Enterprise Information Security at [walter.tong@gta.ga.gov](mailto:walter.tong@gta.ga.gov) for the status of your submitted plan.

Q50: What is a "legitimate" security issue?

A: There several types of "incidents" that can occur within an operational environment. A "legitimate" security issue is any incident that upon examination is determined to be an inadvertent or intentional breach or violation of management, operational and/or technical security policies. Also see Enterprise Incident Response and Reporting Standard for definition of a security incident.

Q51: Where can I get help developing my agency Security Incident Management Plan?

A: Agencies are also strongly encouraged to leverage the guidance provided by NIST Special Pub 800-61 Computer Security Incident Handling Guide <http://csrc.nist.gov/publications/PubsSPs.html> . You may also request a copy of the draft guideline called Incident Response Plans developed to assist agencies with documenting security incident management plans. Send an email to [gta-eis@gta.ga.gov](mailto:gta-eis@gta.ga.gov) to request a copy of the guideline.