REPORT NO. 2013-052
DECEMBER 2012

AGENCY FOR ENTERPRISE INFORMATION TECHNOLOGY

OFFICE OF INFORMATION SECURITY

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE AGENCY FOR ENTERPRISE INFORMATION TECHNOLOGY

Section 14.204, Florida Statutes, creates the Agency for Enterprise Information Technology. The head of the Agency is the Executive Director of the Agency for Enterprise Information Technology. The Executive Director is appointed by the Governor and confirmed by the Cabinet, subject to confirmation by the Senate. David W. Taylor served as the Executive Director during the period covered by our audit.

The audit team leader was Jim Beaumont, CPA, and the audit was supervised by Frank Belt, CPA. Please address inquiries regarding this report to Kathryn Walker, CPA, Audit Manager, by e-mail at kathrynwalker@aud.state.fl.us or by telephone at (850) 487-9085

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

AGENCY FOR ENTERPRISE INFORMATION TECHNOLOGY

Office of Information Security

SUMMARY

This operational audit of the Agency for Enterprise Information Technology (AEIT) focused on an evaluation of the extent to which the AEIT accomplished its responsibilities for information security. Our audit disclosed the following deficiencies:

Finding No. 1: AEIT guidance provided to executive branch agencies (State agencies) did not sufficiently promote compliance with comprehensive risk assessment and security audit requirements of Florida law.

Finding No. 2: The AEIT had not established policies and procedures for the administration of its responsibilities for State agency security plan submissions.

BACKGROUND

The Agency for Enterprise Information Technology (AEIT) was created in 2007 as a separate budget entity within the Executive Office of the Governor. The agency head of the AEIT is the Governor and cabinet. Florida law requires that the AEIT:

- Develop strategies for the design, planning, project management, delivery, and management of enterprise information technology services established in law, including the Statewide e-mail service established in Section 282.34, Florida Statutes.[1]
- Monitor the implementation, delivery, and management of the enterprise information technology services as defined in law.[1]
- Make recommendations to the agency head and the Legislature concerning other information technology services that should be designed, delivered, and managed as enterprise information technology services as defined in law.[1]
- Plan and establish policies for managing proposed statutorily authorized enterprise information technology services, which include:
  - Developing business cases that, when applicable, include the components identified by Florida law;
  - Establishing and coordinating project-management teams;
  - Establishing formal risk-assessment and mitigation processes; and
  - Monitoring the progress of projects.[1]
- Develop, publish, and biennially update a long-term strategic enterprise information technology plan that identifies and recommends strategies and opportunities to improve the delivery of cost-effective and efficient enterprise information technology services to be proposed for establishment pursuant to Florida law.[1]
- Develop information technology standards for the efficient design, planning, project management, implementation, and delivery of enterprise information technology services. [1]
- Provide oversight and recommendations relative to State data center system operations and consolidation.[2]

[1] Section 14.204(4)(a), Florida Statutes.
[2] Section 282.201(2), Florida Statutes.

The amounts appropriated for the operation of the AEIT for the 2010-11 fiscal year totaled $1,367,943, and amounts appropriated for the 2011-12 fiscal year totaled $1,666,826. Authorized positions for the 2010-11 fiscal year totaled 14 and authorized positions for the 2011-12 fiscal year totaled 16.

During the 2012 Legislative session, House Bill 2012-5011 was passed which abolished the AEIT and reassigned functions and duties relating to information technology services coordination, monitoring, and oversight to a new State agency. The Bill also repealed several sections of law including Section 282.34, Florida Statutes, relating to the statewide e-mail service. Consistent with the intent of the legislation, the Legislature did not, for the 2012-13 fiscal year, appropriate moneys for the operation of the AEIT. Appropriations were instead provided for the successor agency. House Bill 2012-5011, was subsequently vetoed by the Governor on April 20, 2012. As a result, the statutes creating the AEIT remained in effect, although moneys to fund the AEIT operations were not appropriated. As of October 12, 2012, the responsibility for the accomplishment of the AEIT's statutory duties and responsibilities had not been reassigned.

FINDINGS AND RECOMMENDATIONS

Relative to information technology security services, Florida law provides that the AEIT is responsible for establishing rules and publishing guidelines for ensuring an appropriate level of security for all data information technology resources of executive branch agencies. More specifically, the AEIT is responsible for the development of enterprise security rules and published guidelines for, among other matters, comprehensive risk analyses, information security audits, and agency security plans.[3] The AEIT is also by law responsible for the development and annual update of an enterprise information security strategic plan.[4]

The rules and guidelines established by the AEIT are to assist agency heads, as well as the AEIT, in meeting information technology security responsibilities assigned by law. Significant agency head responsibilities include the conduct of a comprehensive risk assessment every three years and periodic internal audits and evaluations of the agency's security program for the data, information, and information technology resources of the agency.[5]

Our operational audit of the AEIT focused on an evaluation of the extent to which the AEIT accomplished its responsibilities for information security. As indicated in the succeeding findings, our audit disclosed that the AEIT did not fulfill its responsibilities relative to ensuring an appropriate level of security for data information technology resources of executive branch agencies.

Finding No. 1: Comprehensive Risk Assessment

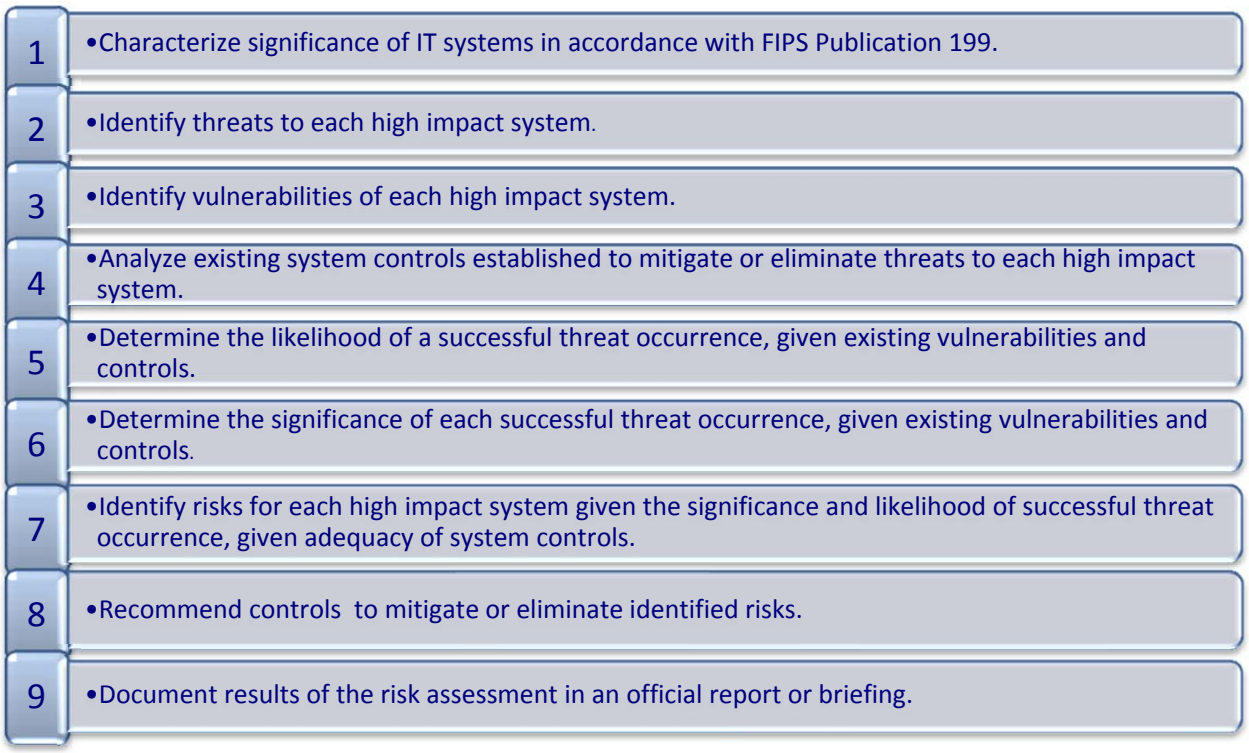
Pursuant to the Federal Information Management Act of 2002 (FISMA), the National Institute of Standards and Technology (NIST) has developed information security standards and guidelines, including minimum requirements, for all Federal agency operations and assets. Federal Information Processing Standards (FIPS) issued by NIST are compulsory for Federal agencies. Special publications are also developed and issued by NIST as recommendations and guidance documents. The AEIT Rules[6] provide that the State use NIST standards and guidance.

[3] Section 282.318(3)(b), Florida Statutes.
[4] Section 282.318(3)(a), Florida Statutes.
[5] Section 282.318(4)(c), Florida Statutes.
[6] Agency for Enterprise Information Technology Rule 71A-1.001(9), Florida Administrative Code.

The AEIT Rules[7] require each agency to categorize its information technology resources according to FIPS Publication 199 as either low impact, moderate impact, or high impact. The impact of an agency's information technology (IT) system is defined as the estimated magnitude of harm that could result from an unauthorized access, modification, destruction, or loss of availability of an IT system or resource. The AEIT Rules also require agencies to implement a documented risk management program, including periodic comprehensive risk assessments, for each of the agency's high impact systems.

According to NIST, the purpose of a comprehensive risk assessment is to identify the threats to and vulnerabilities of an agency's high impact systems, determine whether the agency's existing controls are adequate to address the threats and vulnerabilities, analyze the impact of the threats and vulnerabilities and, when necessary, determine a course of action to mitigate or eliminate those threats and vulnerabilities that are considered unacceptable. Chart 1 below provides the nine-step process necessary to conduct a comprehensive risk assessment consistent with NIST guidelines.

Chart 1
National Institute of Standards and Technology
Risk Assessment Steps



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

As indicated under the **BACKGROUND** heading, Florida law[8] provides that the AEIT is responsible for establishing the rules and guidelines used by agencies to conduct a comprehensive risk assessment and information security audits. To comply with the comprehensive risk assessment requirements, the AEIT developed the 2011 Florida risk assessment survey tool (survey). Each agency's information security manager was ultimately responsible for completing the survey.

[7] Agency for Enterprise Information Technology Rule 71A-1.020, Florida Administrative Code.
[8] Section 282.318(3)(b), Florida Statutes.

According to the survey's instructions, the AEIT's purpose for developing the survey was to help each agency satisfy its 2011 comprehensive risk analysis requirement.[9] However, the survey, in effect, was designed primarily to identify any gaps between the agency's IT policies and those required by the AEIT Rules[10] and did not include the guidance necessary for agencies to conduct a comprehensive risk assessment consistent with NIST's nine-step process (process). For example, while the survey did provide for the categorization of IT systems as either low, moderate, or high impact, the survey's focus was at an agency level, rather than on each significant IT system (step 1 in the process). Also, the survey did not guide agencies to identify and assess the significance, likelihood, and impact of potential threats to and vulnerabilities of the agency's significant IT systems (steps 2, 3, 5, 6, and 7 in the process). The survey also did not provide guidance to agencies relative to the analysis of any existing controls which could mitigate or eliminate identified system threats (step 4 in the process). The guidance in the survey also did not prompt agencies to recommend additional controls to address identified risks and to adequately document the results of the comprehensive risk assessment (steps 8 and 9 in the process).

Incomplete risk assessment guidance may increase the risk that security threats and vulnerabilities will not be addressed by each agency, which can leave agency data and IT resources open to loss, compromise, and misuse. Also, absent sufficiently comprehensive risk assessment guidance, agencies may lack the information necessary to determine the security issues that are to be included in security plans as discussed in finding No. 2.

As noted above, Florida law,[11] as part of the AEIT's responsibility for information technology security services, also required the AEIT to establish rules and guidelines for use by agencies in conducting information security audits. Our audit disclosed that the AEIT had not established such rules and guidelines. Properly performed, a security audit provides assurances of the operational sufficiency and effectiveness of an IT system's security controls, including any controls that were implemented as a result of a comprehensive risk assessment.

Recommendation: Future risk assessment guidance issued by the AEIT or its successor agency should incorporate the methodology included in the applicable NIST publications. Also, rules and guidelines for security audits should be made available to agencies.

Finding No. 2: Submission of State Agency Security Plans

An organization's IT risk management program should include steps to eliminate or mitigate to tolerable levels the risks identified by the comprehensive risk assessment process. The actions needed to mitigate these risks are to be prioritized on an organization's IT security plan (security plan). Florida law[12] requires each State agency to prepare and submit an IT security plan to the AEIT by July 31 of each year. Florida law[13] also requires the AEIT to annually review each State agency's IT security plan.

An agency's security plan is to include both an information security plan (SSP) and an operational information security plan (OSP). The SSP is a three-year plan that defines an agency's security goals, security issues and proposed solutions, and intermediate objectives and projects the costs to implement the agency's risk management program. The OSP is an annual plan that details the activities, timelines, and deliverables the agency has planned for the upcoming fiscal year. The AEIT Rules[14] require each OSP submission include a report on the agency's progress in

[9] Section 282.318(4)(c), Florida Statutes.
[10] Agency for Enterprise Information Technology Rule 71A-1, Florida Administrative Code.
[11] Section 282.318(3)(b), Florida Statutes.
[12] Section 282.318(4)(b), Florida Statutes.
[13] Section 282.318(3)(f), Florida Statutes.
[14] Agency for Enterprise Information Technology Rule 71A-1.003(6), Florida Administrative Code.

addressing matters carried over from prior security plans, a report on related costs that cannot be funded from current resources, and a report summarizing the compensating controls employed by the agency.

Our audit disclosed that the AEIT procedures used in the review of agency security plans were not adequate to provide assurance that the plans were submitted timely and addressed all required elements. Specifically, we found that the AEIT had not developed written procedures to be used in the review of the plans and that the AEIT had not pursued the correction of plan deficiencies.

As part of our audit, we evaluated the timeliness and completeness of the State agency security plan submissions and noted that 17 of the 33 security plans that were to be submitted by July 31, 2011, were not timely received by the AEIT. The plans of 8 agencies had not been received by March 2012, and 9 of the 25 plans which were received were submitted late. The 9 late submissions ranged from 2 to 235 days late, with 5 being over 60 days late. In March 2012, the AEIT sent e-mails requesting that the remaining 8 security plans be submitted.

With respect to the completeness of the 25 security plans that had been submitted, 2 plans (8 percent) did not include the required report describing the progress made since the prior security plan submissions report, no plans (100 percent) included a report on the extent to which if any, that security costs could not be funded from current resources, and 3 plans (12 percent) did not include a summary of the compensating controls employed.

Absent timely submission and adequate review of the State agency security plans, the AEIT lacked the information and ability to meet its IT security planning oversight responsibilities. In particular, absent the receipt of complete and timely agency plans, the AEIT was unable to prepare an accurate and complete State enterprise information security strategic plan. Florida law requires that the AEIT develop, and annually update by February 1, such a plan.

Recommendation: We recommend the AEIT or its successor agency strengthen procedures to ensure timely submission and appropriate review of the State agency IT security plans.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from January 2012 through May 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This operational audit focused on the AEIT's duties and responsibilities relating to the security of the State's data and information technology resources including the 2011 Risk Assessment Surveys and Strategic Information Security Plans. The overall objectives of the audit were:

- To evaluate the effectiveness of established internal controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the relevance and reliability of records and reports; and the safeguarding of assets.

- To evaluate management's performance in achieving compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the relevance and reliability of records and reports; and the safeguarding of assets.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, deficiencies in management's internal controls, instances of noncompliance with applicable governing laws, rules, or contracts, and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of transactions and records. Unless otherwise indicated in this report, these transactions and records were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature, does not include a review of all records and actions of agency management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit we:

- Reviewed for compliance with applicable rules and laws the guidelines provided for the State agencies to conduct comprehensive risk assessments.
- Reviewed the 25 agency risk assessment surveys that had been received by the AEIT as of March 2012 to test compliance with significant governing laws and rules, adequacy of selected controls, and to assess the efficiency and effectiveness of the AEIT's processes to administer its mandated responsibilities.
- Reviewed the 25 State agency security plans that had been received from agencies by the AEIT as of March 2012 to test compliance with significant governing laws and rules, adequacy of selected controls, and to assess the efficiency and effectiveness of the AEIT's process to administer its mandated responsibilities, we
- Performed an analysis to determine whether the AEIT's annual operational work plan was in compliance with Florida Statutes.
- Performed an analysis to determine whether the tasks in the AEIT's annual operational work plan were addressed in the annual report of achievements in accordance with governing Florida Statutes.
- Interviewed applicable AEIT personnel to gain an understanding of the AEIT's role in coordinating the procurement and implementation of a Statewide enterprise email system service required by Section 282.34, Florida Statutes.

- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Interviewed applicable staff within the Executive Office of the Governor to determine as of October 2012, the status of the oversight role and function of the AEIT.
- Discussed with those charged with governance the findings and recommendations that are included in this report and which describe those matters requiring corrective actions.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

As noted under the background heading of this report, funding was not provided for the operations of the AEIT for the fiscal year beginning July 1, 2012. As a result, it was not possible for us to obtain from the audited officials an official response to the findings and recommendations and a description of planned corrective actions.