



Rick Scott, Governor

**State of Florida  
Agency for State Technology**

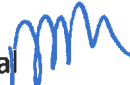
4050 Esplanade Way, Suite 115  
Tallahassee, FL 32399-0950  
Tel: 850-412-6050

Jason M. Allison  
State CIO/Executive Director

---

**MEMORANDUM**

**TO:** Jason M. Allison, State Chief Information Officer/Executive Director  
Melinda M. Miguel, Chief Inspector General, Executive Office of the Governor

**FROM:** Tabitha A. McNulty, Inspector General 

**DATE:** January 27, 2017

**SUBJECT:** Six-Month Status Report to the State of Florida Auditor General Report Number 2017-004

---

Pursuant to section 20.055, Florida Statutes, the following is the six-month status of findings and recommendations included in the Auditor General Report Number 2017-004, *Comprehensive Risk Assessment at Selected State Agencies*, published July 28, 2016.

The review found that management has sufficiently taken corrective action to implement one recommendation and was working to correct the second, as described in the attached report. The Office of Inspector General will no longer monitor finding Number One and will complete a second review of finding Number Two in six months.

If further information is needed, please contact me at 412-6022.

TAM

Attachment

cc: Kathy DuBose, Coordinator  
Joint Legislative Audit Committee (JLAC)  
Sherrill F. Norman, CPA  
State of Florida Auditor General  
Curtis Unruh, Deputy Executive Director  
Danielle Alvarez, Chief Information Security Officer



## Agency for State Technology Office of Inspector General

Jason M. Allison  
State CIO/Executive Director

Tabitha A. McNulty  
Inspector General



### Six-Month Follow-up Response to *Comprehensive Risk Assessment at Selected State Agencies* Auditor General Report Number 2017-004 A-1617-23

#### Overview

Section 20.055, Florida Statutes, requires the Inspector General to monitor and report to the Executive Director and the Chief Inspector General on the status of corrective action taken in response to reports issued by the Auditor General. In July 2016, the Auditor General published Report Number 2017-004, *Comprehensive Risk Assessment at Selected State Agencies*. This audit focused on evaluating selected information technology controls applicable to the comprehensive risk assessment process at six state agencies; the Agency for State Technology (AST) was one of the agencies. Though the report contains multiple findings, only two findings were related to the programs and services within AST.

#### Status Report

##### Finding Number: 1 Comprehensive Risk Assessment Methodology – AST

The risk assessment guidance provided by the AST to the State agencies did not sufficiently promote compliance with the National Institute of Standards and Technology [NIST] risk assessment requirements.

**Recommendation:** We [Auditor General] recommend that the AST incorporate the applicable NIST guidance in the methodology for future State agency risk assessments.

##### Original Response:

The Agency for State Technology (AST) concurs and on March 16, 2016, AST promulgated Rule 74-2, Florida Administrative Code. This Rule incorporated the applicable NIST guidance.

##### Current Status:

Rule 74-2, Florida Administrative Code, was published on March 16, 2016.

**Office of Inspector General Assessment:**

The Office of Inspector General (OIG) finds that the Rule was published in March 2016 and does include NIST Guidance for conducting risk assessments. Additionally, we noted that the Chief Information Security Office has issued a new risk assessment tool to be used by the agencies when communicating risk assessment results back to AST.

Based on the above information, the OIG finds that the recommendations to this finding have been implemented and will no longer follow-up on this finding.

**Finding Number: 2 Comprehensive Risk Assessment Oversight – AST**

The AST's oversight of the State agencies' risk assessments needs improvement to better assist State agencies with the timely submittal of properly completed risk assessments.

**Recommendation:** The AST should develop an effective process for ensuring that State agency risk assessments are timely submitted and that the risk assessments submitted were properly completed and signed by appropriate State agency personnel.

**Original Response:**

AST concurs. AST has drafted a process to track timely submission and completion of agency risk assessments. The final process document will be completed by July 31, 2016, and therefore, will be in place before the next 3-year risk assessment due date.

**Current Status:**

This finding has been addressed. The process was completed and in place prior to the Agency Strategic and Operational Plan (ASOP) assessment being due July 31, 2016.

**Office of Inspector General Assessment:**

The Office of Inspector General (OIG) finds that the Office of Information Security (OIS) issued a procedure for reviewing the Agency Strategic and Operational Plans (ASOP) and the Agency Risk Assessments. The procedure provides guidance on contacting agencies, reminding agencies of submission deadlines, tracking for on-time and/or late submissions, and reviewing the documents completeness.

The OIG reviewed the process used to collect and review the annual ASOP submissions since Agency Risk Assessments have not come due since the issuance of the audit. The process for the two document types are almost identical. Review of the procedure found that it should cover all aspects of the issues noted in the Auditor General's report. However, when the OIG reviewed the actual ASOP submissions we found that:

- Four of the 36 ASOPs received did not have complete cover sheets in the workbook and therefore should have been considered incomplete.
- Three entities were not on the internal tracking spreadsheet used by the OIS to verify timely submissions.

The OIG noted that the OISs constant contact with all the entity's information security managers led to the vast improvement noted from the original finding. Additionally, after speaking with OIS staff, they stated in regards to bullet one, the ASOPs were submitted electronically by a credentialed agency information security manager and are working to verify the missing information from the cover sheets. The OIS will also update the procedure to address the formality of reviewing future document submissions for completeness and indicated that the changes will be completed by February 2017.

The OIG would like to further review this issue in six months and finds that this recommendation is partially implemented and will leave this finding open.

### Objective, Scope, and Methodology

The objective of this follow-up report was to determine the status of action taken by agency management in response to the findings and recommendations made in the Auditor General Report Number 2017-004. The review focused on corrective actions taken since the report's publication on July 28, 2016.

Items reviewed include:

- Florida Administrative Code
- AST procedures for Agency Strategic and Operational Plans and the Agency Risk Assessments
- Interviewing of employees involved in the ASOP reviews
- Review of the ASOPs submitted to AST and the tracking process used

This work product was prepared pursuant to section 20.055, Florida Statutes, and is consistent with the applicable standards as defined in the *Principles and Standards for Offices of Inspectors General* (as published by the Association of Inspectors General) and *International Standards for the Professional Practice of Internal Auditing* (as published by The Institute of Internal Auditors, Inc.)

To promote accountability, integrity, and efficiency in government, the Office of Inspector General conducts audits and reviews of Agency for State Technology's programs, activities, and functions.

Other reports prepared by the Office of Inspector General of the Agency for State Technology may be obtained by telephone (850-412-6022), mail (2585 Shumard Oak Blvd, Tallahassee, FL 32399), or by emailing [Tabitha.McNulty@AST.MyFlorida.com](mailto:Tabitha.McNulty@AST.MyFlorida.com)