From: Clift, Robert <Bob.Clift@dot.state.fl.us>
Sent: Tuesday, January 24, 2017 2:48 PM
To: Boxold, Jim; Miguel. Melinda
Cc: Dubose, Kathy; JLAC; Blackburn, April; Smiley, Greg; Sullivan, Kristofer; McCool, Charles
Subject: Six-Month Update: AG Report 2017-004 IT Operational Audit: Comprehensive Risk Assessments at Selected State Agencies
Attachments: Finding No. 3-Six-Month Update Final.pdf; Finding No 4-Six-Month Update Final.pdf

Chief Inspector General Miguel and Secretary Boxold:

This Six-Month Update is provided for Auditor General report 2017-004[1], an operational audit of Comprehensive Risk Assessments at Selected State Agencies. The two audit recommendations related to the Department are attached above. Corrective actions are in progress for both.

Note for CIG: Your staff will be receiving this report separately using your specified submission protocol.

V/Resp, Bob

ROBERT E. CLIFT
INSPECTOR GENERAL
FLORIDA DEPARTMENT OF TRANSPORTATION
TEL: 850-410-5800| FAX: 850-410-5851
http://www.fdot.gov/ig

1.Section 20.055(6) (h), Florida Statutes, requires a six month status of corrective actions taken as reported to us by the responsible Department of Transportation action officials for the subject audit be provided to "...the agency head or, for state agencies under the jurisdiction of the Governor, the Chief Inspector General on the status of corrective actions taken. The inspector general shall file a copy of such response with the Legislative Auditing Committee."

Auditor General IT Operational Audit of Comprehensive Risk Assessments at Selected State Agencies: Department of Transportation

Response to Finding and Six-Month Update

Finding No. 3: Data Classification, Categorization of IT Systems, and Risk Mitigation

A comprehensive risk assessment includes data classification and categorization of IT systems based on the security objectives of confidentiality, integrity, and availability of information to effectively identify and prioritize IT security controls and IT security control deficiencies. For IT security control deficiencies identified during the risk assessment process, mitigation plans should be developed to resolve or reduce the risks.

For the 3-year risk assessment due March 31, 2015, AHCA, DCF, DEO, DOE, and DOT conducted a risk assessment that included identification of IT security controls and security control deficiencies. However, our examination of the agencies' risk assessment documentation disclosed that the agencies' did not complete the data classification and categorization of IT systems, thereby limiting the effectiveness of an ongoing risk management program and the development of security plans. Specifically, we found that the agencies:

- Specialized security awareness training was limited without the classification of data, including identification of confidential and exempt data that required specialized training.
- Audit logging and monitoring was limited without the identification of confidential and exempt data that requires logging and monitoring of access and transactions involving such data.
- Analysis of configuration management IT security controls for IT systems was ineffective without the classification of data and categorization of IT systems.
- Disaster recovery planning was less effective without the categorization of IT systems.
- IT security controls over backup resources were less effective without the identification of confidential and exempt data.
- Data loss prevention and incident response was limited without the identification of confidential and exempt data that should be monitored for loss or unauthorized access.

Additionally, AHCA, DOE, and DOT did not developed risk mitigation plans for all IT security control deficiencies identified in the risk assessment process. The lack of data classification and categorization of IT systems and risk mitigation plans may reduce the agencies' assurance that risks and all likely threats and vulnerabilities have been identified and evaluated, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to mitigate through appropriate IT security controls, and which residual risks to formally accept.

Recommendation: To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Agency Response and Corrective Action Plan:

Agree. A risk assessment for Fiscal Year 2016-2017 has been funded by the Legislature. During this risk assessment, the classification of data and the categorization of IT systems will be included in the project scope. FDOT is working to develop formal risk management processes and governance. Risk mitigation will be part of that project.

Six-Month Update:

The previous response is still in progress. FIPS 199 categorization is being used with the Security Plan process to identify the criticality of systems and data based on the level of confidentiality, integrity and availability.

Auditor General IT Operational Audit of Comprehensive Risk Assessments at Selected State Agencies: Department of Transportation

Response to Finding and Six-Month Update

Finding No. 4: IT Security Controls

IT security controls are safeguards and countermeasures prescribed for information systems or organizations that are designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems or organizations and satisfy a set of defined security requirements. According to the NIST framework, IT security controls include critical IT functions and activities. Such IT functions and activities include security awareness training, logging and monitoring, configuration management, standards for identification and authentication, disaster recovery planning, data loss prevention and incident response planning, and ongoing risk management.

Our review of selected IT security controls at AHCA, DCF, DEO, DOE, and DOT disclosed that some IT security controls need improvement. Specifically, we found that:

1. While the DOT had implemented Office of Information Systems (OIS) Method and Practice documents for baseline hardening, written policies and procedures that enforced the use of the OIS Method and Practice documents were not in place.
2. Additionally, while the DOT had a documented change control process that required configuration changes for systems and applications to be approved, the process did not require verification of the systems and applications configurations to the baseline prior to implementation.
3. While the DOT had a DR plan for critical IT resources and annually tested the DR plan for the mainframe, annual testing of the DR plan was not always performed for other critical IT resources.
4. The DOT had not developed system security plans for all DOT systems.
5. Certain IT security controls related to audit logging and monitoring need improvement. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising DOT data and IT resources. However, we have notified appropriate DOT management of the specific issue.

The lack of appropriate IT security controls increases the risk that the confidentiality, integrity, and availability of agency data and IT resources may be compromised.

Recommendation: To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.

Agency Response and Corrective Action Plan:

1. Agree. The OIT will develop policies and procedures that enforce the use of the OIT methods and practices by June 30, 2017.

2. Agree. The OIT is currently in the process of implementing a change control process that will include the verification of the systems and applications configurations to the baseline prior to implementation. This will be a multi-phased project with the first phase to be completed by June 30, 2017.

3. Agree. The Department agrees that some critical IT resources were not included in the DR plan testing, however, this was due to a lack of available funds and staff resources. If the resources needed are made available, the Department will develop a process for testing the DR plan that includes these critical IT resources. OIT is unable to provide a completion date at this time because it is not known when, if ever, the Legislature will approve the financial resources needed to complete the DR process.

4. Agree. The Department is currently working to identify those systems that currently have no security plan. Once identified, security plans will be developed for those systems. The initial phase of this project is the identification of those systems that currently have no security plan. This phase of the project is to be done by June 30, 2017.

5. Agree. The Department is working to correct items reported for logging and monitoring.

Six-Month Update:

1. Update: The OIT is working on the development of policies and procedures that will enforce the use of OIT methods and practices. This is still on track to be completed by June 30, 2017.

2. Update: The OIT is working on the implementation of the change control process previously mentioned. This is still on track to be completed by June 30, 2017.

3. Update: The previous response still applies. The Legislature has, to date, not approved the financial resources required to complete the DR process.

4. Update: The Department is working to identify those systems that currently have no security plan. This phase of the project is on track to be completed by June 30, 2017.

5. Update: The Department is working to update its policies and procedures to be in compliance with Chapter 74-2, F.A.C. Chapter 74-2, F.A.C. is based upon the NIST framework. This will be included in the Department's Strategic Plan currently being developed which will cover the next 3-5 years of planned work. This will be a multi-phased project. The first phase, which is the original assessment, is to be completed by February 2017. The next phase will be the development of the implementation plan.