Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

ANANTH PRASAD, P.E.
SECRETARY

October 12, 2011

Ananth Prasad, P.E.
Secretary of Transportation
Department of Transportation
605 Suwannee Street, MS 57
Tallahassee, FL 32399-0450

RE: **Auditor General Report No. 2011-174**
Financial Management (FM) System –
Information Technology Operational Audit
August 2010 through November 2010

Dear Secretary Prasad:

As required by Section 20.055(5)(h), Florida Statutes, attached is the six month status report for the subject audit. The report details the implementation or current status of each recommendation.

If you have any questions, please call me at 410-5823.

Sincerely,

Robert E. Clift,
Inspector General

REC:tw

Enclosure

cc: Joint Legislative Auditing Committee

FLORIDA DEPARTMENT OF TRANSPORTATION

6-month Follow-up Response to the Auditor General's Financial Management (FM) System – Information Technology Operational Audit August 2010 through November 2010 Report #2011-174

Finding No. 1: Timely Disabling of Access Privileges

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, the Department did not timely disable network, mainframe, and database access privileges of some former and reassigned employees. Additionally, the Department was unable to provide us a list of terminated contractors and, therefore, could not demonstrate that terminated contractors' access privileges were timely disabled.

Recommendation: The Department should ensure that network, mainframe, and database access privileges are disabled in a timely manner. Additionally, the Department should develop procedures to create and maintain a listing of former contractors to ensure that access privileges are timely disabled. Furthermore, the Department should improve its review of access privileges to increase the likelihood of timely detecting access privileges that are no longer necessary because of employee terminations or reassignments.

Initial Response: We concur with the findings. From the result of the audit, it is obvious that there was a flaw in our process for revoking and removing access in a timely fashion. As a result we have implemented an automated notification to critical teams (Database and Server) when terminations occur. These notifications are validated by both teams to ensure that no lingering access remains.

The Information Technology Assurance and Security Management (ITASM) team has discussed the need to work with project managers to verify the contractors start and end dates and to back-load that information as received. The back-loading of the contract dates for consultant accounts into Automated Access Request Form system (AARF), coupled with a recertification, should address this issue.

Current Response: The Department has scheduled an application recertification for completion by end of the first quarter in 2012. The task of back-loading contractors into the Automated Access Request Form system will be a task assigned as a result of this recertification.

Anticipated Completion Date: March 30, 2012

Finding No. 2: Appropriateness of Access Privileges

Some users had inappropriate or unnecessary access privileges to the FM System application, database, and production datasets. Similar issues were noted in prior audits of the Department, most recently our report No. 2010-095.

Recommendation: The Department should limit access privileges to include only the individuals who need the access privileges in the performance of their job duties. Additionally, the Department should implement procedures to routinely monitor and adjust access privileges, including those of SSRC employees, in the event of employee terminations, reassignments, or changes in job functions.

Initial Response: We concur with the findings. To minimize the potential risks of future issues, ITASM will work with the Financial Management (FM) application owners to review current access processes and procedures. Based on this review the ITASM team, working with the FM application owners, will implement improved notification processes and appropriate changes. The ITASM team will also work with the FM application owners to determine the appropriate interval for the recertification of FM access. The ITASM team and the FM application owners will work together to implement recertification for the FM system processes at the interval which appropriately reflects the security requirements of the application.

Current Response: The Department has scheduled an application recertification for completion by end of the first quarter in 2012.

Anticipated Completion Date: March 30, 2012

Finding No. 3: Access Control Records Retention

Contrary to the requirements of the State of Florida General Records Schedule for the retention of access control records, the Department did not retain some network and mainframe access control records.

Recommendation: The Department should ensure that access control records are retained as required by the General Records Schedule.

Initial Response: We concur with the findings. To comply with the State of Florida General Records Schedule for the retention of access control records, ITASM is working to implement statewide event tracking and mainframe logging alerts and reports. As the event records are received by Florida Department of Transportation (FDOT) Security, the necessary validation will be performed. The access control records will then be maintained by FDOT Security for the time required by the General Records Schedule.

Current Response: The product Event Tracker, for active directory monitoring, was successfully implemented statewide in June 2011. Logs are being reviewed as needed. The product Vanguard Reporter, used for mainframe / RACF, is installed and configuration and testing is underway. The Vanguard Reporter's implementation is expected to be completed at the end of December.

Anticipated Completion Date: December 30, 2011

Finding No. 4: Security Controls

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, certain Department network, mainframe, and data center security controls related to the FM System needed improvement.

Recommendation: The Department should improve its network, mainframe, and data center security controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Initial Response: We concur with the findings and will take appropriate corrective actions to improve IT security controls which ensure the continued confidentiality, integrity and availability of Department data and IT resources.

Current Response: The Department successfully implemented, statewide, a procedure that facilitates monitoring, escorting and logging of all visitors entering the Department's data centers. The Department continues to review its existing controls and modify when needed.

Completed Date: September 13, 2011

Finding No. 5: Program Change Controls

For two FM System program changes, the Department could not provide documentation of testing and approval of program changes, respectively, although required by its program change control procedures.

Recommendation: The Department should ensure that its program change control procedures for unit testing of application components and approval of program changes for production are consistently followed to provide increased assurance of the integrity of program changes being moved into the production environment.

Initial Response: We concur with the findings. Our change control procedure requires testing and review as part of the workflow before requesting the user to test and approve. It currently does not require written documentation of the developer's unit test. The addition of this requirement will be included during the next review of the procedure. The email that showed the appropriate approval for the referenced change could not be located when requested by this audit, but was found and provided later (March 30, 2011). In the future, we will ensure written approvals are properly filed so that they may be readily obtained for audit purposes.

Current Response: The Office of Information Systems (OIS), with Department management support, is working towards the implementation of an OIS Operational Manual, which will incorporate our existing internal procedures. The noted update to our change control procedure will be included. It will also include the use of documentation for end user testing and approval, prior to promoting code to production. We hope to have the change control procedure implemented as part of the OIS Operations Manual no later than July 1, 2012.

Anticipated Completion Date: July 1, 2012

Finding No. 6: IT Policies

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, some Department IT policies were outdated.

Recommendation: The Department should update its IT policies and periodically review the appropriateness of the policies to ensure that management's current expectations regarding IT controls are being accurately communicated to employees.

Initial Response: We concur with the findings. To comply, updates are currently being performed. The specific documents cited in the audit have been prioritized. Work has begun to revise Information Technology (IT) policies and procedures affected by Chapter 71, Florida Administrative Code (71-FAC).

Current Response: The specific documents cited in the audit have been completed and were communicated to staff on June 15, 2011. The Department continues to review policies for compliance to 71-FAC.

Completed Date: June 15, 2011

Finding No. 7: Security Awareness Training Program

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, the Department's security awareness training program needed improvement with regard to providing periodic refresher training to remind employees and contractors of their security responsibilities.

Recommendation: The Department should continue with its efforts to implement, within its security awareness training program, provisions for ongoing security awareness training to ensure that employees and contractors are reminded of their responsibilities for maintaining the confidentiality, integrity, and availability of Department data and IT resources.

Initial Response: We concur with the findings. The ITASM team has been developing a Security Awareness Computer Based Training (CBT) suite for the past several months. The program is supported by management and will include a policy which will require all staff to have annual security awareness training.

Current Response: The ITASM team completed a Security Awareness CBT and received approval from the Department's management to allow this to be part of required annual training. This CBT is being rolled out as part of the annual Cyber Security Month. The Department supports Cyber Security Month by holding informational kiosks and providing helpful material as well as monthly newsletters on the importance of information technology security awareness.

Completed Date: September 6, 2011

Finding No. 8: Positions of Special Trust

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, the Department had not designated all positions having sensitive IT responsibilities and elevated access privileges as positions of special trust or performed level 2 background screenings on all employees occupying the positions.

Recommendation: The Department should review its positions with sensitive IT responsibilities and elevated access privileges, consider designating such positions as positions of special trust, and perform the required level 2 background screenings on employees occupying the positions.

Initial Response: We concur with the findings. We understand the finding regarding positions of special trust. With that in mind, Nelson Hill, the Chief Information Officer (CIO) is working with Department management, Personnel, and the General Council to review the issue and to establish a department policy regarding positions of special trust.

Once the process has been approved, the CIO will work with Department management, Personnel, and the General Council to identify which positions would be classified as positions of special trust and which IT positions might be subject to level two background checks.

Current Response: The issues related to designating positions of special trust is being considered in conjunction with changes to IT staffing as a result of data center consolidation and position reductions. We hope to have a definitive direction established on this no later than July 1, 2012.

Anticipated Completion Date: July 1, 2012