Florida Department of Transportation

CHARLIE CRIST
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

STEPHANIE C. KOPELOUSOS
SECRETARY

August 27, 2010

Stephanie C. Kopelousos
Secretary
Department of Transportation
605 Suwannee Street
Tallahassee, Florida 32399-0450

RE: **Auditor General Report No. 2010-095**
Financial Management (FM) System –
Information Technology Operational Audit
July 1, 2008 through June 30, 2009

Dear Secretary Kopelousos:

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,

Ron Russo
Inspector General

RR: tw

Enclosure

cc: Kathy DuBose, Staff Director
Cathy Boyett
Joint Legislative Auditing Committee
JLAC@leg.state.fl.us

Florida Department of Transportation
Office of Inspector General

Source of Audit:	Auditor General
Report Number:	2010-095
Report Title:	Financial Management (FM) System – Information Technology Operational Audit July 1, 2008 through June 30, 2009

Finding No. 1: IT Policies and Procedures

Our audit disclosed that certain Department IT policies were outdated. Specifically:

- The Department's Internet site, FDOT Information Security Administration, referenced the Information Resource Security Policy from the State Technology Council, 1998. The State Technology Council no longer exists and the document is over ten years old. In addition, another statutory reference included on the Internet site no longer exists.

- The Department's policy, Electronic Security for Public Records, dated November 29, 1993, and the document, Custodian and Owner Responsibilities – Data & Software, dated January 19, 1995, included a reference to Information Resource Commission Rule 44-4, Florida Administrative Code, Information Resource Security Standards and Guidelines that was repealed in June 1998.

Our audit further disclosed that the Department did not have written procedures for performing emergency program changes.

Recommendation: The Department should update its IT policies and periodically review the ongoing appropriateness of the policies to ensure that management's current expectations regarding IT controls are being communicated to employees. The Department should also establish written emergency program change procedures to ensure that management's expectations for performing emergency changes are clearly understood and consistently followed.

Initial Response: We concur with the finding. In regards to the Department's Internet site, the references have been corrected. Department's Standard Operating System, Topic No. 025-020-002-I, dated December 20, 2007, provides a uniform system for developing, maintaining and providing access to the Department's procedural documents. Responsibility for this process has been reviewed and assigned to IT Assurance and Security Management staff. Furthermore, as part of the Business Systems Support Office's ongoing effort to improve their Change Management processes, they will create documentation for the implementation of emergency program changes.

Current Response: Emergency program changes are initiated and resolved through the FDOT Service Desk process. BSSO has documented how service desk requests are prioritized in the "BSSO Request Classifications" document. Based on this document, emergency program changes are given the highest priority. This document is currently being used by our programmers and will act as a framework for developing a department-wide emergency change management procedure. We expect to have draft documentation ready for an audit review no later than September 30, 2010.

This procedure will be added to the library of Department IT policies and procedures, which is currently being updated by a review team that consists of OIS management and the recently hired (in April 2010) Quality Review Specialist. The “OIS Procedures and Directives Internal Review Process” document has been updated and adopted to reflect the internal process that will be used by the team when reviewing internal and Departmental IT policies and procedures. The management team and the Quality Review Specialist have performed a precursory review of the Department IT policies and procedures and removed those that were deemed obsolete. This group has proceeded with updating the remaining documents to reflect management’s current expectations regarding IT controls.

Source of Audit:	Auditor General
Report Number:	2010-095
Report Title:	Financial Management (FM) System – Information Technology Operational Audit July 1, 2008 through June 30, 2009

Finding No. 2: Security Awareness Training Program

Other than newsletters and weekly security tips by Computer Security Administration, the Department has no program for ongoing security awareness training that included employee and contractor acknowledgement of security responsibilities in writing on an annual basis, as similarly noted in our report No. 2007-183.

Recommendation: The Department should continue with its efforts to implement an ongoing comprehensive security awareness training program to ensure that all employees and contractors are aware of the importance of information handled and their responsibilities for maintaining its confidentiality, integrity, and availability. Additionally, the Department should require all employees and contractors to acknowledge their understanding and acceptance of security-related responsibilities on an annual basis.

Initial Response: We concur with the findings and will continue to pursue having a policy which will require all staff to have security awareness training every three years. OIS Internal Procedure Elevated Computer Security Access, Topic No. 325-A60-307-a, dated July 8, 2007, requires an annual certification for OIS personnel with elevated accesses in conjunction with the annual employee evaluation process.

Current Response: OIS continues to provide timely updates on computer security awareness through a monthly security newsletter, weekly security tips and planned quarterly updates to the Executive Committee. Completion of the Computer Security Awareness Computer Based Training is required for all new employees before access to internal computer resources is provided.

An internal review of other available options to expand awareness training has taken place. Following discussion with the FDOT Information Security Manger, the Chief Information Officer has scheduled discussions with FDOT Executive Management and the FDOT Personnel Officer on August 30th, 2010 to address the best way to implement mandated security awareness training. This may involve requiring employees to retake the CBT module periodically as a refresher on security awareness. We will develop a strategy and a plan to go forward no later than October 31st, 2010. The plan will articulate processes and timelines for completion. Including mandatory security awareness training as a part of new employee orientation with cyclical training will be a key recommendation.

Florida Department of Transportation
Office of Inspector General

Source of Audit:	Auditor General
Report Number:	2010-095
Report Title:	Financial Management (FM) System – Information Technology Operational Audit July 1, 2008 through June 30, 2009

Finding No. 3: Positions of Special Trust

OIS had officially designated only three positions as positions of special trust. Two of the positions were IT technology staff assigned to support the Office of Motor Carrier Compliance and the third position was the OIS Personnel Liaison. Other employees within OIS, including security, system, and database administrators, had been assigned sensitive IT responsibilities and granted elevated access privileges that indicated a need for them to be subject to security background checks. However, they had not been officially designated as positions of special trust or subjected to background checks or fingerprinting.

Recommendation: The Department should, as a part of its review of policy regarding positions of special trust, consider designating other IT positions with sensitive responsibilities and elevated access privileges as positions of special trust.

Initial Response: We concur with the findings. As stated the Chief Information Officer has initiated discussion with the Department's Personnel Office concerning this matter for consideration at a policy level within the Department. Until this issue is resolved at a policy level, the Office of Information Systems (OIS) will continue to require of OIS personnel, and all consultants and contractors working in OIS as contract workers, to acknowledge their understanding of the responsibilities inherent in having elevated computer security access as documented in OIS Internal Procedure Topic No. 325-A60-307-a dated July 8, 2007.

Current Response: The Chief Information Officer has scheduled additional discussions with FDOT Executive Management and the FDOT Personnel Officer on August 30th, 2010 to formulate a strategy regarding positions of special trust within the IT workforce. Department direction concerning this matter will be established from those discussions with an action plan and timeline.

Source of Audit:	Auditor General
Report Number:	2010-095
Report Title:	Financial Management (FM) System – Information Technology Operational Audit July 1, 2008 through June 30, 2009

Finding No. 4: Security Controls - Network and Mainframe

Our audit disclosed certain network and mainframe security controls related to the FM System that needed improvement. Similar issues were noted in our report No. 2007-183. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should improve its network and mainframe 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 corrective action or acknowledge the acceptance of any associated risks.

Current Response: The implementation of the Automated Access Request Form (AARF) system has significantly improved the effectiveness of user access controls. Implementation included a recertification of all staff access in the Department. To strengthen these controls security awareness training and quarterly security status reports will be aimed at changing the Management culture as it relates to access and privileges. This effort will enable Management to be cognizant of approvals and authorizations based upon the least amount of access needed for the performance of duties. The IT Assurance and Security Management (ITASM) team will continue to evaluate the effectiveness of the procedures and make appropriate adjustments as needed.

Source of Audit:	Auditor General
Report Number:	2010-095
Report Title:	Financial Management (FM) System – Information Technology Operational Audit July 1, 2008 through June 30, 2009

Finding No. 5: Timely Removal of Former and Reassigned Employee Access

As similarly noted in our report No. 2007-183, the Department did not remove the network and mainframe access privileges of some former employees in a timely manner.

Recommendation: The Department should ensure that FM System and network access privileges of former employees are removed in a timely manner.

Initial Response: We concur with the findings. The user implementation of the Automated Access Request Form system provides a convenient and effective mechanism for management to report terminations. AARF automates the distribution of termination notices to all owners of that users security accesses. Additionally, the Office of Comptroller can provide a termination report and the AARF administrators will monitor the termination notices.

Current Response: The implementation of the Automated Access Request Form (AARF) system has significantly improved the effectiveness of user access termination process. For the last 6 months, the Office of Comptroller has provided the IT Assurance and Security Management (ITASM) with termination reports which are now being validated on a monthly basis. This revised process is working well. We will continue to monitor and review the effectiveness of the procedures and make appropriate adjustments as needed.

Completed: 6/30/2010

Source of Audit:	Auditor General
Report Number:	2010-095
Report Title:	Financial Management (FM) System – Information Technology Operational Audit July 1, 2008 through June 30, 2009

Finding No. 6: Database and Production Access Privileges

As similarly noted in our report No. 2007-183, some inappropriate or unnecessary access privileges existed to the database and production level object programs, increasing the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

Recommendation: The Department should periodically review the ongoing appropriateness of access to the database and the production-level object libraries to ensure that access privileges are timely removed or adjusted as necessary.

Initial Response: We concur with the finding. All identified issues have been resolved. The Office of Comptroller is now providing a termination report and the AARF administrators will monitor the termination notices for FM accesses. The IT Assurance and Security Management (ITASM) team will work with the FM application owners to develop and implement an access recertification process.

Current Response: With the completion of the implementation of the Automated Access Request Form (AARF) system, we have completed a Department-wide recertification of all user access. With this phase completed, IT Assurance and Security Management (ITASM) staff will begin the process of developing a recurring recertification process. The plans to enhance Management's awareness of security and access privileges will strengthen the certification review and approval process.