REPORT NO. 2010-095
FEBRUARY 2010

DEPARTMENT OF TRANSPORTATION

FINANCIAL MANAGEMENT (FM) SYSTEM

Information Technology Operational Audit

For the Period
July 1, 2008, Through June 30, 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF TRANSPORTATION

Pursuant to Section 20.23(1)(a), Florida Statutes, the Secretary of the Department of Transportation is appointed by the Governor and subject to confirmation by the Senate. Stephanie C. Kopelousos served as Secretary during the audit period.

The audit team leader was Bill Tuck, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF TRANSPORTATION

Financial Management (FM) System

SUMMARY

The Department of Transportation (Department) is a public works agency responsible for the development and maintenance of Florida's transportation system. Annually, the Department prepares, by way of a revision, the Five-Year Work Program pursuant to Section 339.135, Florida Statutes. This document is to be a balanced financial plan that provides a list of transportation projects (by phase) that are scheduled for implementation during the ensuing five-year period. The Work Program includes all proposed project commitments classified by major program and appropriation category. The Department uses the Financial Management (FM) System to manage and track work project progress; seek Federal authorization, participation, and reimbursement; and monitor financial commitments to transportation projects.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to the FM System during the period July 1, 2008, through June 30, 2009, and determining the status of corrective actions regarding prior audit findings disclosed in our report No. 2007-183.

The results of our audit are summarized below:

Finding No. 1: Some Department IT policies were outdated and the Department lacked written procedures for performing emergency program changes.

Finding No. 2: As similarly noted in our report No. 2007-183, the Department's ongoing security awareness training program needed improvement.

Finding No. 3: The Department had not designated certain positions having sensitive IT responsibilities and elevated IT access privileges as positions of special trust.

Finding No. 4: Certain network and mainframe security controls at the Department related to the FM System needed improvement. Similar issues were disclosed in our report No. 2007-183.

Finding No. 5: As similarly noted in our report No. 2007-183, the Department did not timely remove the FM System access privileges of some former employees.

Finding No. 6: As similarly noted in our report No. 2007-183, some users had inappropriate or unnecessary access privileges to the database and production-level object libraries.

BACKGROUND

The FM System is composed of four subsystems: the Work Program Administration Subsystem (WPA), the Project Cost Management Subsystem (PCM), the Federal Authorization Management System (FAMS), and the Federal Programs Management Subsystem (FPM). WPA provides the ability to plan, implement, and track the progress of the Department's Work Program. PCM provides a mechanism to monitor the Department's commitments. FAMS transmits Federal project information to the Federal Highway Administration (FHWA) for subsequent authorization of Federal funding for transportation projects. FPM is used to manage and seek reimbursement for projects that are eligible for FHWA participation.

The FM subsystems exchange information with various State and Federal information systems. PCM interfaces with the State's accounting system, FLAIR, and is the repository of actual project cost historical information. FAMS interfaces with the Federal Fiscal Management Information System for management of Federal authorizations, and

FPM interfaces with the Federal Rapid Approval and State Payment System for transmission of periodic billings for Federal reimbursement.

The FM System was developed and is maintained in-house by the Business Systems Support Office within the Office of Information Systems (OIS). It runs on a mainframe computer and FM System users connect to the mainframe through the Department's network.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: IT Policies and Procedures

Management is responsible for developing and maintaining policies to support IT strategy. These policies include policy intent, roles, and responsibilities; compliance; and references to procedures and guidelines that address key topics such as security, internal controls, and integrity and confidentiality of data.

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. Emergency IT changes were referenced in the Department's Information System Development Methodology (ISDM), and an internal process for making emergency program changes was in place. However, there were no written procedures that described the internal process to be followed. In response to audit inquiry, Business System Support Office staff indicated that emergency program changes is an area that they are working on to improve and formalize.

Without current, written policies and procedures, the risk is increased that IT controls will not be followed consistently and in a manner pursuant to management's expectations.

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.

Finding No. 2: Security Awareness Training Program

Department of Management Services Rule 60DD-2.001(3), Florida Administrative Code, provides that each agency shall develop, implement, and maintain an information resource security program that produces a documented, ongoing training program for information resource security awareness. In Topic No. 325-060-555-a, Access to the Department's Computer Network Resources, the Department required security awareness training as part of the process for gaining access to IT resources. However, other than newsletters and weekly security tips by Computer

Security Administration, there was 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. The Department acknowledged the need for an ongoing security awareness training program and developed a draft policy addressing it, but had not approved and implemented the policy. A comprehensive security awareness training program would decrease the risk that the Department's IT resources may be intentionally or unintentionally compromised by employees or contractors while performing their assigned duties.

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.

Finding No. 3: Positions of Special Trust

Section 110.1127(1), Florida Statutes, provides that each employing agency shall designate those employee positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment. Section 435.04(1), Florida Statutes, provides that all employees in positions designated by law as positions of trust or responsibility shall be required to undergo security background investigations, referred to as level 2 background screenings, as a condition of employment and continued employment. The level 2 background screenings are to include fingerprinting for all purposes, Statewide criminal and juvenile records checks through the Florida Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation. In addition, Department of Management Services Rule 60DD-2.008(2)(c), Florida Administrative Code, provides that background investigations are required for personnel in positions of special trust or for those having access to sensitive locations.

In July 2007, OIS adopted internal procedure 325-A60-307-a, Elevated Computer Security Access. The purpose of this procedure was to establish a process for OIS personnel, and all consultants and contractors working in OIS as contract workers, to acknowledge their understanding of the responsibilities inherent in having elevated IT access privileges. This procedure defined what constituted elevated access. However, the procedure did not associate the elevated access with the special trust designation.

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. Without appropriate background screening, including fingerprinting, the risk is increased that a person with an inappropriate background could be employed in a position with sensitive IT responsibilities and be provided access to and misuse critical IT resources. In response to audit inquiry, Department management stated that 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.

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.

Finding No. 4: Security Controls - Network and Mainframe

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain network and mainframe security controls related to the FM System that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department staff of the specific issues. 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.

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

Effective security-related policies regarding access privileges are critical to effective information system security. Effective policies include ensuring that IT management removes IT access privileges of former and reassigned employees in a timely manner. Department policy as provided in Topic No. 325-060-555-a, Access to the Department's Computer Network Resources, required prompt action to be taken in removing the IT access privileges of former employees.

FM System access privileges are granted through the use of network and mainframe accounts. 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.

Specifically, our test of 481 former and reassigned employees' network and mainframe access privileges for the period July 1, 2008, through June 30, 2009, disclosed that 2 former employees, who separated from employment on October 1, 2008, and November 28, 2008, continued to have update access privileges to the network for 330 and 259 days, respectively, after employment separation. Additionally, a former employee who separated from employment on May 29, 2009, continued to have update mainframe access privileges to the WPA Subsystem of the FM System for 83 days after employment separation. Our review of Department records indicated that none of the 3 former employees had accessed the network or the FM System since their separation date.

By not timely removing a former employee's access privileges to the Department's IT resources, the risk is increased that the access privileges may be misused by the former employee or others.

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

Finding No. 6: Database and Production Access Privileges

Effective management of access privileges is intended to ensure that employees and contractors are restricted from performing incompatible functions or functions beyond their responsibility and that the access privileges of former or reassigned employees and contractors are timely removed or adjusted as appropriate. 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.

Some database access privileges were assigned at the user group level and all user IDs attached to user groups automatically inherited the group access privileges. Other user IDs had been established that had individually assigned access privileges. Our test of the appropriateness of database access privileges of nine user groups and 24 user IDs with individually assigned access privileges, as of August 5, 2009, and August 10, 2009, respectively, disclosed the following:

- Five of the nine user groups' access included in our test had database update and administrator access that Department staff had determined, in response to audit inquiry, was not needed.
- The remaining four user groups included 15 user IDs that had been granted unnecessary update access. Specifically, 13 of the 15 user IDs had formerly been used for system processes but were no longer being used. The remaining 2 user IDs belonged to a former employee who, according to Department staff, had separated from employment on February 28, 2004. In response to audit inquiry, Department staff indicated that they have begun to remove the unnecessary access.
- Five of the 24 user IDs included in our test with individually assigned access privileges had update access that was no longer needed. Three of the user IDs had formerly been used for system processes. The remaining 2 user IDs belonged to a Department employee and a contractor who no longer needed the access to perform their job duties. The Department was unable to provide specific dates upon which the employee and contractor no longer needed the access privileges. In response to audit inquiry, Department staff removed all unnecessary access for these two individuals.
- One of the 24 user IDs included in our test was assigned to a former employee. The database access privileges assigned to the former employee remained active for 28 days after employment separation, at which time access was removed by Department staff in response to audit inquiry. Department staff further indicated that the former employee's database access privileges had not been used after separation.

Our test of the appropriateness of access privileges to the production-level object libraries, as of August 5, 2009, disclosed that 6 of the 31 user IDs included in our test with update access privileges to production objects belonged to former or reassigned employees or contractors. In response to audit inquiry, the Department subsequently removed the access privileges of the 6 user IDs. For 5 of the 6 user IDs, the access privileges had remained active for 36 to 241 days after separation from employment, reassignment to other Department positions where the access privileges were no longer needed, or termination of contractual services. For the remaining user ID, Department staff could not determine the date that the contractual services were terminated or the length of time that the access privileges remained active after termination. In response to audit inquiry, Department staff indicated that the access privileges associated with the 6 user IDs had not been used after reassignment or separation.

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.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2007-183.

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 IT operational audit in accordance with applicable 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.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. Additional objectives were to determine whether the reporting mechanisms within the FM System, such as data exception or unusual activity reporting, were effective in maintaining the reasonableness of its data and to determine whether management has corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2007-183.

The scope of our audit focused on evaluating selected IT controls applicable to the FM System during the period July 1, 2008, through June 30, 2009.

In conducting our audit, we:

- Interviewed Department personnel.
- Evaluated the effectiveness of selected controls to determine the effectiveness of selected application access controls programmed within the FM System.
- Obtained an understanding of the Department's data exception and unusual activity reporting, operating system access and security controls, and FM System application controls.
- Evaluated the effectiveness of selected security administration controls including the development and implementation of a comprehensive information resource security program.
- Evaluated the appropriateness of selected controls for non-Department-owned computers connecting to the network.
- Evaluated the effectiveness of selected controls to ensure proper identification of positions of special trust within the Office of Information Systems.
- Evaluated the effectiveness of selected controls to ensure an ongoing security awareness training program.
- Observed and tested the effectiveness of access controls over the application, database, network, and host operating system, including user identification and authentication.
- Observed and tested the effectiveness of logical access controls established for the application, including appropriate password conventions and settings and security controls.

- Observed and tested the effectiveness of controls to ensure timely removal of IT access privileges of terminated or transferred employees.
- Observed and tested the effectiveness of controls to ensure timely monitoring of security event and violation logs.
- Evaluated the appropriateness of selected controls to ensure equipment, such as wireless access points, had the latest software releases that include security feature enhancements and patches.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated February 10, 2010, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

Florida Department of Transportation

CHARLIE CRIST
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

STEPHANIE C. KOPELOUSOS
SECRETARY

February 10, ~~2009~~ 2010 sw

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

I am pleased to respond to the preliminary and tentative audit findings and recommendations concerning the audit of:

Financial Management (FM) System
Information Technology Operational Audit
July 1, 2008 through June 30, 2009

As required by Section 11.45(4)(d), Florida Statutes, our responses to the findings are enclosed.

I appreciate the efforts of you and your staff in assisting to improve our operations. If you have any questions, please contact our Inspector General, Ron Russo, at 410-5823.

Sincerely,

SCKopel

Stephanie C. Kopelousos
Secretary

SCK:tw

Enclosure

cc: Ron Russo, Inspector General

www.dot.state.fl.us

RECYCLED PAPER

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT OF TRANSPORTATION

Response to the Auditor General's Preliminary and Tentative Audit Findings and Recommendations

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.

Management 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.

Finding No. 2: 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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Management 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.

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.

Management 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.

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.

Management Response:

We concur with the findings and will take corrective action or acknowledge the acceptance of any associated risks.

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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Management 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.

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.

Management 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.