REPORT NO. 2011-174
APRIL 2011

DEPARTMENT OF TRANSPORTATION

FINANCIAL MANAGEMENT (FM) SYSTEM

Information Technology Operational Audit

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 period of our audit.

The audit team leader was Faye Smith, CISA, and the audit was supervised by Shelly Posey, 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) 487-9175; 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 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 of the FM System focused on evaluating the effectiveness of selected general and application information technology (IT) controls applicable to the FM System. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2010-095.

The results of our audit are summarized below:

Finding No. 1: 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.

Finding No. 2: 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.

Finding No. 3: 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.

Finding No. 4: 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.

Finding No. 5: 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.

Finding No. 6: As similarly noted in prior audits of the Department, most recently our report No. 2010-095, some Department IT policies were outdated.

Finding No. 7: 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.

Finding No. 8: 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.

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 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). FM System users connect to the mainframe through the Department's network. In July 2009, the FM System mainframe was moved to the Southwood Shared Resource Center (SSRC) and the remaining IT equipment within the Burns Building Data Center is scheduled to be moved to the SSRC by March 2012.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Timely Disabling of Access Privileges

Effective management of system access privileges includes provisions to timely disable a user's access privileges when employment termination, job reassignment, or contract termination occurs. In addition, Department 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 and reassigned employees.

FM System access privileges are granted through the use of network and mainframe accounts. As similarly noted in prior audits of the Department, most recently our report No. 2010-095, the Department did not disable the network and mainframe access privileges of some former and reassigned employees in a timely manner, as described in the following paragraphs. The existence of the former and reassigned employees' access privileges indicated a need for improved Department review of access privileges and increased the risk that access privileges could be misused by former employees or others.

Upon audit request, the Department provided us a list of 482 employees who terminated from or were reassigned within the Department during the period January 1, 2010, through September 23, 2010. Our comparison of this list to user access privileges within the network and mainframe disclosed that some access privileges were not timely disabled. Specifically:

- Thirty-three network user accounts had not been disabled as of the date of our testing on September 23, 2010, and had remained active from 6 to 244 days after the date the employee terminated or transferred.

- Forty-two mainframe user accounts had not been revoked (disabled) as of the date of our testing on September 23, 2010, and had remained active from 6 to 265 days after the dates the employees terminated or transferred.

Through additional audit procedures, we noted that four former employees' mainframe user accounts were not disabled. As of the date of our test (October 7, 2010), the access privileges of the four former employees had remained active from 22 to 1,925 days after their terminations.

Other audit procedures disclosed five former employees who retained access privileges to FM System databases by being members of groups with update access privileges. Specifically, four former employees' user identification codes (IDs) retained update access privileges to FM System production tables and one former employee's user ID retained systems authorities for the database. In response to audit inquiry, the Department provided documentation that the five former employees' user IDs with inappropriate update access privileges had been disabled on November 17, 2010, by removing the user IDs from the groups with the update access privileges. As of the date of disabling, the access privileges of the five former employees had remained active from 63 to 1,966 days after their terminations.

Upon audit inquiry, the Department was unable to determine whether the former and reassigned employee access privileges described above had been used after the dates of termination or reassignment because the Department had not retained the access control records of the employees. This matter is discussed further in Finding No. 3.

Furthermore, the Department was unable to provide us a listing of former contractors for the period January 1, 2010, through September 24, 2010. As a result, the Department could not demonstrate that the former contractors' access privileges had been 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.

Finding No. 2: Appropriateness of Access Privileges

Effective management of access capabilities is intended to ensure that employees and contractors only have the access privileges needed to perform their duties and access is restricted to prevent a user from performing incompatible functions or functions beyond the user's responsibilities. As discussed in the following paragraphs, some inappropriate or unnecessary access privileges existed for the FM System application, database, and production datasets, increasing the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

FM System Application

Our review of 172 FM System users with update access privileges to selected FM System functions disclosed that 7 users had multiple user IDs in the System. Although the access privileges associated with these multiple user IDs were appropriate based on the users' job functions, the existence of the multiple user IDs was not necessary to grant the users the required access and increased the risk that some of the IDs may be overlooked should the users' access privileges need to be disabled. In addition, 8 users had inappropriate update access privileges for their job functions. In response to audit inquiry, Department management provided documentation indicating that 3 of the 8 users with inappropriate access privileges had been removed from the applicable access group as of November 3, 2010.

Database

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, some inappropriate or unnecessary access privileges existed for the database. Some database access privileges were assigned at the user group level and all user IDs attached to the user group automatically inherited the user group's access privileges. Our testing of the appropriateness of database access privileges of seven user groups as of September 20, 2010, disclosed that two of the seven user groups' access privileges were inappropriate. Specifically:

- One user group was a test group that had inappropriate update access privileges to FM System production tables. In response to audit inquiry, the Department provided documentation that this user group was removed on December 2, 2010.
- One user group was no longer needed and had inappropriate update access privileges to an FM System production table. In response to audit inquiry, the Department provided documentation that this user group was removed on December 21, 2010.

Additionally, 26 user IDs attached to four of the seven user groups had inappropriate access privileges. Specifically:

- Seven employees had multiple user IDs with duplicate access privileges. In response to audit inquiry, Department management provided documentation that the seven employees' user IDs with duplicate access privileges were removed on November 17, 2010.
- Six user IDs with update access privileges to an FM System production table had inappropriate access privileges for their job functions. In response to audit inquiry, Department management provided documentation that five of the user IDs were removed on December 2, 2010, and the other user ID was removed on December 21, 2010.
- One user ID with systems authorities for the database had inappropriate access privileges for his job functions. In response to audit inquiry, Department management provided documentation that the user ID's systems authorities were removed on November 17, 2010.
- Twelve user IDs with systems authorities for the database were obsolete user IDs that were no longer needed. These 12 user IDs belonged to two user groups. In response to audit inquiry, Department management provided documentation that the user IDs were removed from both groups on December 21, 2010.

Production Datasets

As similarly noted in prior audits of the Department, most recently our report No. 2010-095, our review of the appropriateness of mainframe security access privileges for FM System production datasets, including FM System programs, data, and job control language, disclosed some inappropriate access privileges. Specifically:

- Two of four consultants who had the ability to modify production datasets did not require the access privileges for their job functions. Both consultants had required the access privileges at an earlier point in time; however, the privileges were no longer required for their job functions.
- Eight of 13 employees who had the ability to modify production datasets did not need the access privileges for their job functions.
- Seven of 19 SSRC employees who work on the FM System mainframe with the ability to modify production datasets had access privileges that were not required for their job functions. Additionally, 2 of the 7 employees had terminated employment with the SSRC on December 31, 2009; however, their access privileges had not been removed as of the date of our test (October 12, 2010).
- Eight of 22 system IDs with the ability to modify production datasets were unnecessary and not being used by the Department.

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.

Finding No. 3: Access Control Records Retention

The *State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies* (General Records Schedule), revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. Contrary to the General Records Schedule requirements, the Department did not retain some network and mainframe access control records. Without the adequate retention of access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements.

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

Finding No. 4: Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain network, mainframe, and data center 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 management and staff of the specific issues. Without adequate network, mainframe, and data center security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that the Department's data and IT resources may be subject to improper disclosure, modification, or destruction.

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.

Finding No. 5: Program Change Controls

Effective controls over changes to programs are intended to ensure that only authorized and properly functioning changes are implemented. Department Topic 325-A80-501-a, Production Migration of Computer Application Components, provides that computer application components will be tested by the OIS staff in a unit test environment and that the Functional Application Coordinator or Application Owner is responsible for approving the program change for production.

Our review of a sample of 30 FM System program changes implemented between January 1, 2010, and September 1, 2010, disclosed two changes for which the Department was unable to provide documentation that some requirements outlined in its program change control procedures were followed. Specifically, one program change lacked documentation of unit testing by the OIS application developer and the other change lacked documentation that the change was approved for production by the Financial Application Coordinator or Application Owner.

Without testing and approval of program changes, the risk is increased that unauthorized or erroneous programs may be moved into the production environment without timely detection.

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.

Finding No. 6: IT Policies

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. As similarly noted in prior audits of the Department, most recently our report No. 2010-095, the Department had not updated some IT policies presented on its Internet and Infonet (intranet) sites. Specifically:

- The Department's Infonet site referenced the Information Resource Security Policy from the State Technology Council, 1998. The State Technology Council no longer exists and the Policy is no longer in effect.
- The Department's Electronic Security of Public Records Policy, located on the Department's Internet site, included as an authoritative source Information Resource Commission Rule 44-4, Florida Administrative Code, Information Resource Security Standards and Guidelines. This Rule was repealed in June 1998. The document, which also included multiple incorrect statutory references, is used as a part of the Department's new employee security awareness training course that is conducted online.

Without current, written policies, 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 appropriateness of the policies to ensure that management's current expectations regarding IT controls are being accurately communicated to employees.

Finding No. 7: Security Awareness Training Program

An effective security awareness program includes first-time training for new employees and contractors and periodic refresher training for all employees and contractors that apprises or reminds users of the importance of preserving the confidentiality, integrity, and availability of data and IT resources entrusted to them. Department Topic 325-060-555-a, Access to the Department's Computer Network Resources, required security awareness training as part of the process for gaining access to IT resources.

Aspects of the Department's security awareness training program needed improvement. As similarly noted in prior audits of the Department, most recently our report No. 2010-095, other than a monthly newsletter and weekly security tips, the Department did not provide ongoing (periodic refresher) security awareness training to employees and contractors. The lack of periodic refresher security awareness training increases the risk that employees and contractors may inadvertently compromise the security of Department data and IT resources.

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.

Finding No. 8: Positions of Special Trust

Section 110.1127(1), Florida Statutes, states that each employing agency shall designate those positions, that because of 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 and continued employment. Section 435.04(1)(a), Florida Statutes, provides that a level 2 background screening should include, but is not limited to, fingerprinting for Statewide criminal history record checks through the Department of Law Enforcement and national criminal history record checks through the Federal Bureau of Investigation and may include local criminal records checks though local law enforcement agencies.

In response to our request for OIS positions designated as special trust positions, Department management stated that four OIS positions had been designated as requiring background checks**.** The Department performed level 2 background screenings on three of the employees; however, a level 1 background screening, which did not include fingerprinting, was performed on the fourth employee. Also, the sensitive responsibilities and elevated access privileges of other positions, such as security administrators for the Central and District offices and database administrators, indicated a need for these positions to be subject to background screenings. Without appropriate background screening, including fingerprinting, the risk is increased that an employee with an inappropriate background could be employed in a position with sensitive IT responsibilities and be provided access to and misuse critical IT resources.

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.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for a few of the issues included in our report No. 2010-095. Corrective actions were not taken for most of the prior audit findings as described in the findings above.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public agency 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 from August 2010 to November 2010, and performed selected audit procedures from January 2010 through December 2010, 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 audit were to determine the effectiveness of selected IT controls applicable to the FM System 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; the safeguarding of IT resources; the effectiveness and efficiency of IT operations; and whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2010-095.

The scope of this audit focused on evaluating selected IT controls applicable to the FM System, including selected general IT controls over systems development and modification, computer operations, logical access to programs and data, and physical and security safeguards. The audit also included selected application IT controls and selected user controls applicable to the FM System.

In conducting our audit, we:

- Interviewed Department personnel.
- Observed and evaluated the effectiveness of key processes and procedures related to the FM System.
- Observed and evaluated the effectiveness of selected input, processing, and output controls, as well as exception reporting and manual follow-up procedures for the FM subsystems. As part of the evaluation, we tested the proper functioning of 30 significant FM subsystem input edits.
- Observed and evaluated the effectiveness of controls surrounding the transfer of data between FM subsystems and other applications, including reconciliation processes and procedures.
- Observed and evaluated the effectiveness of selected logical access controls in ensuring that access privileges to the FM System application, network, database, job control language, and operating system, including user identification and authentication was appropriately restricted and provided an adequate separation of duties.
- Evaluated the effectiveness of controls for timely disabling the access privileges of terminated or reassigned employees. Specifically, we reviewed a list of 482 employees who terminated from or were reassigned within the Department during the period of January 1, 2010, through September 23, 2010, to determine if the network and mainframe access privileges were timely disabled.
- Tested the effectiveness of selected controls over the authorization, testing, approval, and documentation of 30 FM System program changes implemented between January 1, 2010 and September 1, 2010.
- Observed and evaluated the appropriateness of selected control activities surrounding backup and recovery procedures for FM System data and program files.
- Observed and evaluated the adequacy of physical security controls to IT resources located within the Department's facilities.
- Determined whether the Department had an ongoing security awareness training program in place.

  Determined whether IT positions with sensitive responsibilities and elevated access privileges had been designated as positions of special trust and whether level 2 background screenings had been performed for employees filling those positions.

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 April 8, 2011, the Acting 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

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

OFFICE OF THE
SECRETARY

April 8, 2011

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
August 2010 through November 2010

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, Bob Clift, at 850-410-5800.

Sincerely,

Francis B. Gibbs
Acting Secretary

FBG:tw

Enclosure

cc: Robert E. Clift, Inspector General

www.dot.state.fl.us

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

August 2010 through November 2010

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.

Management 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.

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.

Management 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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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.

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.

Management 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.

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.

Management 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.

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.

Management 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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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.

Management 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).

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.

Management 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.

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.

Management 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 FDOT 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 FDOT 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.