REPORT NO. 2015-039
NOVEMBER 2014

DEPARTMENT OF TRANSPORTATION

PROJECT COST MANAGEMENT SUBSYSTEM (PCM)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF TRANSPORTATION

The Department of Transportation was created pursuant to Section 20.23, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. Ananth Prasad served as Secretary during the period of our audit.

The audit team leader was Debra Clark, CPA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF TRANSPORTATION

Project Cost Management Subsystem (PCM)

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, a five-year work program pursuant to Section 339.135, Florida Statutes. Section 339.135(3)(a), Florida Statutes, states that the tentative and adopted work programs shall be based on a complete, balanced financial plan and shall set forth the proposed commitments and planned expenditures, respectively, of the Department classified by major program and fixed capital appropriation categories to accomplish the objectives of the Department. To help accomplish this, the Department uses the Project Cost Management Subsystem (PCM) to provide cost-related data for the Department; store project-related Florida Accounting Information Resource Subsystem (FLAIR) transactions; allocate FLAIR transactions to work program funds; monitor the cost-transfer process; provide transaction edits for specific Department-related errors and exceptions; provide users with the capability to submit batch update jobs; and validate work activity at the phase, program, and financial project levels.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to the PCM. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2011-174 that were applicable to the scope of this audit.

Our audit disclosed areas in which improvements in PCM IT controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: The Department had not updated the PCM application security plan to ensure that it was current and provided an overview of the PCM security requirements and the controls in place or planned for meeting those requirements.

Finding No. 2: The Department could not provide, upon audit inquiry, authorization documentation of PCM user access privileges for 11 users included in our test of user access authorizations.

Finding No. 3: The Department had not performed a review of PCM user access privileges since 2011.

Finding No. 4: Certain Department security controls related to PCM user authentication needed improvement.

Finding No. 5: Department security awareness training procedures needed improvement to ensure that all employees completed security awareness training in a timely manner.

Finding No. 6: The Department had not maintained application design documentation for the PCM during the period of our audit.

BACKGROUND

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. The PCM is a subsystem of the Department's FM System. The PCM is the primary interface for the Department with FLAIR and is the repository of actual project cost historical information. The PCM also provides cost-related data for the Department; stores project-related FLAIR transactions; allocates FLAIR transactions to work program funds; monitors the cost-transfer process; provides transaction edits for specific Department-related errors and exceptions; provides users with the capability to submit batch update jobs; and validates work activity at the phase, program, and financial project levels.

The PCM is a mainframe system that was developed and is maintained in-house by the Business Systems Support Office within the Office of Information Systems. PCM users connect to the mainframe through the Department's network. The Department's mainframe environment, infrastructure, and backup servers are housed and supported at the Southwood Shared Resource Center.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Application Security Plan

Effective application security management provides a foundation for entity management to obtain reasonable assurance that an application is effectively secure. As such, security management controls include, among other things, the establishment of an application security plan. The application security plan documents a summary of the security requirements for the application and describes the security controls in place or planned for meeting those requirements. Application security plans require periodic review, modification, and plans of action for implementing security controls.

Department management indicated, upon audit inquiry, that an application security plan was created when the Department developed the PCM many years ago but that it had not been updated to include the details that would be expected in a current application security plan, such as an overview of the security requirements of the application and a description of all of the controls in place or planned for meeting those requirements. Without an up-to-date PCM application security plan, the risk is increased that the Department may not implement adequate security controls over the application and that inappropriate application access and compromised data confidentiality, integrity, and availability may occur.

Recommendation: The Department should update the PCM application security plan to ensure that it is current and provides an overview of the security requirements and the controls in place or planned for meeting those requirements.

Finding No. 2: Access Authorization Documentation

Effective access authorization controls include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. In December 2009, the Department completed the implementation of the Automated Access Request Form (AARF) to initiate and track authorizations of requests for user access privileges. Prior to the implementation, access authorizations for the PCM were processed through electronic mail.

During our audit, we requested AARFs or other authorization documentation for 15 PCM user accounts to determine if the access privileges granted were appropriately authorized. Department staff provided AARFs; however, as similarly noted in our report No. 2011-174, for 11 of 15 user accounts the AARFs did not show authorization of the access privileges to the PCM. Of these 11 AARFs, 6 pertained to user accounts that had been granted access privileges before the implementation of AARFs and 5 pertained to user accounts that had been granted access privileges subsequent to the implementation of AARFs.

The absence of documentation of management's authorization of PCM user account access privileges may limit the Department's ability to ensure that access privileges granted to PCM users are authorized by management for the accomplishment of assigned job duties.

Recommendation: The Department should document management's authorization of PCM user account access privileges to ensure that access privileges are appropriately authorized.

Finding No. 3: Periodic Review of User Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Our audit disclosed that the Department had not performed a review of PCM user access privileges since 2011. The lack of access authorization documentation as noted in Finding No. 2 above also indicates that the Department was not performing such periodic reviews. Without the periodic review of user access privileges, the risk is increased that inappropriate user access privileges may exist and not be timely detected.

Recommendation: The Department should perform periodic reviews of PCM user access privileges to ensure the continued appropriateness of assigned user access privileges.

Finding No. 4: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that certain Department security controls related to PCM user authentication needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising PCM data and IT resources. However, we have notified appropriate Department management of the specific issues. Similar issues were also communicated to Department management in connection with prior audits of the Department, most recently our report No. 2011-174.

The lack of appropriate security controls related to user authentication increases the risk that the confidentiality, integrity, and availability of PCM data and IT resources may be compromised.

Recommendation: The Department should improve PCM user authentication controls to ensure the continued confidentiality, integrity, and availability of PCM data and IT resources.

Finding No. 5: Security Awareness Training Procedures

AEIT Rules 71A-1.008(1) and (2), Florida Administrative Code, provide that the agency Information Security Manager shall implement and maintain an agency information security awareness program and that, at a minimum, agency workers shall receive annual security awareness training.

As similarly noted in prior audits of the Department, most recently our report No. 2011-174, our audit disclosed that the Department's security awareness training procedures needed improvement to ensure that all employees completed security awareness training in a timely manner. We noted that, as of June 30, 2014, security awareness training records indicated that 9 of 184 employees included in our review were between 65 and 256 days overdue for annual security

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

awareness training and the records for 2 of the 184 employees did not indicate any security awareness training having been completed.

Without adequate security awareness training procedures to ensure that all employees complete the training in a timely manner, the risk is increased that employees may inadvertently or intentionally compromise the security of the PCM or other IT resources.

Recommendation: The Department should improve its security awareness training procedures to ensure that all Department employees complete such training in a timely manner.

Finding No. 6: Application Design Documentation

AEIT Rule 71A-1.015(1), Florida Administrative Code, states that an agency shall ensure information technology resources are correctly maintained to ensure continued confidentiality, availability, and integrity. Application design documentation provides the basis for validating that the design of the application meets management's requirements and that control objectives applicable to the application controls of the system ensure the confidentiality, availability, and integrity of data. Continued maintenance of application design documentation helps ensure that changes to the original application design continue to align with management's requirements and control objectives to ensure the confidentiality, availability, and integrity of data.

Upon audit inquiry, we determined that the Department had not maintained detailed application design documentation for the PCM. Department staff had drafted an *FDOT Financial Management Scope Study* (*Study*) with a draft date of June 16, 2014. The goal of the *Study* was to aid the Department in identifying the full scope of the Department's financial management needs to decide which systems and business processes should be included in the scope for the development of the functional requirements of the future FM Suite. The draft *Study* provided PCM design documentation at a high-level. Without detailed PCM design documentation, the risk is increased that the PCM may not function as intended by management and that appropriate controls may not be in place to ensure the confidentiality, availability, and integrity of PCM data.

Recommendation: The Department should maintain application design documentation for the PCM to ensure the confidentiality, availability, and integrity of PCM data.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for one of the four findings included in our report No. 2011-174 that were applicable to the scope of this audit. Corrective actions were not taken for one of the four prior audit findings as described in the findings above. In addition, two prior audit findings were only partially corrected. Four prior audit findings included in our report No. 2011-174 were not in the scope of this audit.

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 from May 2014 through July 2014 in accordance with 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. An additional objective was to determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our audit report No. 2011-174 that were within the scope of this audit.

The scope of our audit focused on evaluating selected business process application controls over transaction data input, processing, and output, applicable to the PCM, during the period July 2013 through June 2014 and selected actions through July 9, 2014. The audit also included selected application-level general IT controls over security management, logical access to programs and data, configuration management, and contingency planning.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this IT operational audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the purpose and goals of the PCM.
- Obtained an understanding of the Department's IT functions as they related to the PCM.
- Obtained an understanding of data input (internal and external), processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of data input into the PCM.

- Observed selected general, application, and user controls, including policies, procedures, hardware, and software, related to the PCM.
- Observed and evaluated selected transaction data input, processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of PCM data.
- Evaluated application security management controls related to the PCM, including the application security plan and security awareness training. Specifically, we reviewed the training records of 184 employees to determine if security awareness training was completed in a timely manner.
- Evaluated the effectiveness of selected access controls to ensure that access privileges to the PCM were appropriately authorized. Specifically, we reviewed the access authorization forms as of July 9, 2014, for 15 of 88 users who had PCM user accounts as of June 30, 2014, to determine that the access privileges were authorized.
- Evaluated the effectiveness of selected user authentication controls for the PCM. Specifically, we reviewed Department policies and other documentation regarding authentication settings and reviewed the authentication settings to determine if the settings were sufficient to restrict access.
- Evaluated the effectiveness of security event logging and monitoring related to the PCM. Specifically, we reviewed security procedures utilized for reporting logged security events and we reviewed a sample of security events that were logged and reported.
- Evaluated the effectiveness of selected logical access controls including periodic reviews for the PCM to ensure that user access privileges were appropriately restricted and provided an adequate separation of duties. Specifically, we reviewed user access privileges of 83 users as of April 21, 2014.
- Evaluated application configuration management controls related to the PCM, including access to move programs to the production environment.
- Evaluated contingency planning controls related to the PCM.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those matters requiring corrective action.

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 November 5, 2014, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

ANANTH PRASAD, P.E.
SECRETARY

November 5, 2014

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

Dear Mr. Martin:

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

Department of Transportation – Information Technology Operational Audit
Project Cost Management (PCM) Subsystem

As required by Section 11.45(4)(d), Florida Statutes, the Department's response to the operational audit findings is enclosed.

If you have any questions, please contact our Inspector General Bob Clift, at 850-410-5800.

I appreciate the efforts of you and your staff in assisting to improve our operations.

Sincerely,

Ananth Prasad, P.E.
Secretary

AP: cm

cc: Brian Peters, Assistant Secretary
Tom McCullion, Chief Information Officer
Robin Naitove, Comptroller
Robert E. Clift, Inspector General
Kristofer Sullivan, Director of Audit

www.dot.state.fl.us

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Auditor General IT Operational Audit of the Department of Transportation Project Cost Management Subsystem (PCM)

Response to Finding

Finding No. 1: The Department had not updated the PCM application security plan to ensure that it was current and provided an overview of the PCM security requirements and the controls in place or planned for meeting those requirements.

Recommendation: The Department should update the PCM application security plan to ensure that it is current and provides an overview of the security requirements and the controls in place or planned for meeting those requirements.

Agency Response and Corrective Action Plan: The Department agrees with this finding. The Department's Office of Information Systems shall document a systems security plan for PCM.

Estimated Corrective Action Date:

04/24/2015

Agency Contact and Telephone Number:

Tom McCullion, Chief Information Officer 850-414-4771

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Auditor General IT Operational Audit of the Department of Transportation Project Cost Management Subsystem (PCM)

Response to Finding

Finding No. 2: The Department could not provide, upon audit inquiry, authorization documentation of PCM user access privileges for 11 users included in our test of user access authorizations.

Recommendation: The Department should document management's authorization of PCM user account access privileges to ensure that access privileges are appropriately authorized.

Agency Response and Corrective Action Plan: The Department agrees with this finding. The Department's Office of Information Systems and Office of Comptroller shall work together to backload PCM users to the Department's Automated Access Request Form System. All future requests for PCM access shall be requested through the Automated Access Request Form System.

Estimated Corrective Action Date:

01/16/2015

Agency Contact and Telephone Number:

Tom McCullion, Chief Information Officer 850-414-4771

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Auditor General IT Operational Audit of the Department of Transportation Project Cost Management Subsystem (PCM)

Response to Finding

Finding No. 3: The Department had not performed a review of PCM user access privileges since 2011.

Recommendation: The Department should perform periodic reviews of PCM user access privileges to ensure the continued appropriateness of assigned user access privileges.

Agency Response and Corrective Action Plan: The Department agrees with this finding. During the execution of the PCM Audit, the Office of Information Systems was in the process of conducting a review of PCM user access privileges. The review of PCM user access privileges officially concluded on 09/10/2014 and the results of review, along with the actions taken, was delivered to the Department's Office of Inspector General.

Estimated Corrective Action Date:

09/10/2014

Agency Contact and Telephone Number:

Tom McCullion, Chief Information Officer 850-414-4771

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Auditor General IT Operational Audit of the Department of Transportation Project Cost Management Subsystem (PCM)

Response to Finding

Finding No. 4: Certain Department security controls related to PCM user authentication needed improvement.

Recommendation: The Department should improve PCM user authentication controls to ensure the continued confidentiality, integrity, and availability of PCM data and IT resources.

Agency Response and Corrective Action Plan: The Department agrees with this finding. The Department's Office of Information Systems has a project planned to improve PCM user authentication controls to ensure the continued confidentiality, integrity, and availability of PCM data and IT resources.

Estimated Corrective Action Date:

06/30/2015

Agency Contact and Telephone Number:

Tom McCullion, Chief Information Officer 850-414-4771

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Auditor General IT Operational Audit of the Department of Transportation Project Cost Management Subsystem (PCM)

Response to Finding

Finding No. 5: Department security awareness training procedures needed improvement to ensure that all employees completed security awareness training in a timely manner.

Recommendation: The Department should improve its security awareness training procedures to ensure that all Department employees complete such training in a timely manner.

Agency Response and Corrective Action Plan: The Department agrees with this finding. On October 17th, 2014, the Department's Office of Information Systems initiated a project to assess the efficacy of the Office of Information System's training program, document the process controls in place for training, and to establish a standard process control for training. Upon the establishment of documented and standardized process controls, the Office of Information Systems shall incorporate the training into its quality assurance review program.

Estimated Corrective Action Date:

12/03/2014

Agency Contact and Telephone Number:

Tom McCullion, Chief Information Officer 850-414-4771

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Auditor General IT Operational Audit of the Department of Transportation Project Cost Management Subsystem (PCM)

Response to Finding

Finding No. 6: The Department had not maintained application design documentation for the PCM during the period of our audit.

Recommendation: The Department should maintain application design documentation for the PCM to ensure the confidentiality, availability, and integrity of PCM data.

Agency Response and Corrective Action Plan: The Department agrees with this finding. It is the Department's Office of Information Systems' expectation that the PCM system will be included within the scope of the Work Program Integration Initiative project. Application design documentation for the PCM system shall be created and maintained upon the re-writing of the PCM system.

Estimated Corrective Action Date:

11/30/2017

Agency Contact and Telephone Number:

Tom McCullion, Chief Information Officer 850-414-4771