Centennial
FDOT
1915★2015

Florida Department of Transportation

RICK SCOTT
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

JIM BOXOLD
SECRETARY

April 29, 2015

Mr. Jim Boxold
Secretary
Department of Transportation
605 Suwannee Street
Tallahassee, Florida 32399-0450

RE: **Auditor General Report No. 2015-039**
Information Technology Operational Audit
Department of Transportation
Project Cost Management Subsystem

Dear Secretary Boxold:

As required by Section 20.055(5) (h), Florida Statutes, attached is the six month status of corrective actions taken as reported to us by the responsible action officials for the subject audit. This update details the implementation or current status of the audit recommendation for our agency. This six-month update will also be filed with the Joint Legislative Auditing Committee, as required by statute.

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

Sincerely,

Robert E. Clift

Robert E. Clift
Inspector General

RC:cm

Attachments

cc: Joint Legislative Auditing Committee- Kathy Dubose, Staff Director
Chief Inspector General's Office- Melinda Miguel, Chief Inspector General
Department of Transportation- Mike Dew, Chief of Staff

FLORIDA DEPARTMENT OF TRANSPORTATION
6-month Follow-up to the
Office of the Auditor General
Information Technology Operational Audit- Department of Transportation
Project Cost Management Subsystem
Report No. 2015-039

Finding No. 1: The Department had not updated the PCM IT 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.

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.

Audit Response: The Department agrees with this finding. The Department's Office of Information Systems shall document a systems security plan for PCM.

6-month Follow-up Response:

As of April 2015, the security plan for PCM had not been developed. However, the project to develop the security plan for PCM has been initiated and will be completed by May 29, 2015.

FLORIDA DEPARTMENT OF TRANSPORTATION
6-month Follow-up to the
Office of the Auditor General
Information Technology Operational Audit- Department of Transportation
Project Cost Management Subsystem
Report No. 2015-039

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.

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.

Audit Response: 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.

6-month Follow-up Response:

As of the date of this response, the project to backload PCM users to the Department's Automated Access Request Form System (AARF) is in progress with an anticipated completion date of June 2015.

Also, AARF now manages access requests for PCM.

FLORIDA DEPARTMENT OF TRANSPORTATION
6-month Follow-up to the
Office of the Auditor General
Information Technology Operational Audit- Department of Transportation
Project Cost Management Subsystem
Report No. 2015-039

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

Agency for Enterprise Information Technology (AEIT) 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.

Audit Response: The Department agrees with this finding. During the execution of the PCM Audit, the Office of Informations Systems was in the process of conducting a review of PCM user access privileges. The review of PCM user access privileges officially concluded on 9/10/2014 and the results of the review, along with actions taken, was delivered to the Department's Office of Inspector General.

6-month Follow-up Response:

Complete.

FLORIDA DEPARTMENT OF TRANSPORTATION
6-month Follow-up to the
Office of the Auditor General
Information Technology Operational Audit-Department of Transportation
Project Cost Management Subsystem
Report No. 2015-039

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

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.

Audit Response: 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.

6-month Follow-up Response:

Complete.

FLORIDA DEPARTMENT OF TRANSPORTATION
6-month Follow-up to the
Office of the Auditor General
Information Technology Operational Audit-Department of Transportation
Project Cost Management Subsystem
Report No. 2015-039

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

Agency 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 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.

Audit Response: 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.

6-month Follow-up Response:

Complete.

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

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.

Audit Response: 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.

6-month Follow-up Response:

As of April 2015, the Work Program Integration Initiative project has been initiated. The rewrite of PCM falls within the scope of this project. However, the project is in the very early stages with an anticipated completion date 3-4 years in the future. The application design documentation for PCM will be developed at the time of the rewrite of the system. The anticipated completion date of this project is Fiscal Year 2018/2019.