STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-206
June 2017

DEPARTMENT OF TRANSPORTATION

Federal Programs Management Subsystem

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Transportation

The Department of Transportation is established by Section 20.23, Florida Statutes. The head of the Department is the Secretary of Transportation who is appointed by the Governor and subject to confirmation by the Senate. Jim Boxold served as Department Secretary during the period of our audit.

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Arthur Hart, CPA.

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 are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF TRANSPORTATION

Federal Programs Management Subsystem

SUMMARY

This operational audit of the Department of Transportation (Department) focused on evaluating selected information technology (IT) application and general controls applicable to the Federal Programs Management subsystem (FPM) and included a follow-up on finding No. 4 in our report No. 2015-039. Our audit disclosed the following:

Finding 1: Department procedures did not provide for comprehensive and timely periodic reviews of application user access privileges and the Department had not performed a review of FPM user access privileges since May 2015 or reviews of other system access privileges since June 2013.

Finding 2: Department access controls need improvement to ensure that access granted is properly authorized and documented.

Finding 3: The access privileges for some FPM, Financial Management common database, and FPM production dataset users did not restrict users to only those functions necessary for their assigned job duties.

Finding 4: Some Department access controls related to the configuration management system need improvement to promote an appropriate separation of duties.

Finding 5: Department procedures defining the requirements for obtaining and removing access to the Department's IT resources need improvement.

Finding 6: Certain Department security controls related to FPM user authentication and logging and monitoring for FPM data and related IT resources need improvement.

BACKGROUND

The Financial Management (FM) Suite is the Department of Transportation's (Department) primary financial management system for planning, managing, financing, and budgeting transportation projects. The FM Suite integrates common data used by the major subsystems that support the core financial and project management business processes of the Department. The FM Suite comprises the Work Program Administration subsystem (WPA), Federal Authorization Management System, Project Cost Management subsystem, and the Federal Programs Management subsystem (FPM). This audit focused on the FPM.

The FPM provides the ability to manage and seek reimbursement for projects that are eligible for Federal Highway Administration (FHWA) participation. The FPM supports Department activities to:

- Track appropriations and obligating authority, Federal billing, and vouchering.
- Interface with the Federal Management Information System to manage Federal appropriations.
- Generate periodic billing for Federal reimbursement from the FHWA.

FINDINGS AND RECOMMENDATIONS

Finding 1: Periodic Access Review

Agency for State Technology (AST) rules[1] require agency control measures to address responsibilities of information stewards that facilitate periodic reviews of access rights with information owners. The frequency of the reviews must be based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

As part of our audit, we evaluated Department procedures and made inquiries with Department management related to the performance of periodic reviews of user access privileges, including review of FPM user access privileges. Our audit procedures disclosed that, although the Department had established procedures[2] requiring, for specified systems (e.g., network identity management systems), the respective information technology (IT) resource owners to perform annual reviews (recertification) of user access privileges, annual recertifications of the specified systems had not been performed since June 2013.

We also noted that Department procedures did not address a process for application owners to review the user access privileges for each application (e.g., FPM). In response to our inquiry, Department management indicated that application owners are responsible for determining the recertification requirements for their applications. Department management further stated that application recertification information is not automatically provided as part of the annual recertification effort, but is provided to an application owner if requested. We also noted that the Department had not performed a review of FPM user access privileges since May 2015.

Without comprehensive and timely periodic reviews of system and application user access privileges, management's assurance that user access privileges to IT resources are authorized and appropriate is limited.

Recommendation: We recommend that Department management improve controls and enhance Department procedures to require the performance of periodic reviews of user access privileges granted for all Department applications. We also recommend that Department management ensure that annual recertifications of system user access privileges are performed as required by Department procedures.

Finding 2: Access Authorization Documentation

AST rules[3] require each agency to manage identities and credentials for authorized devices and users and establish control measures that address responsibilities of information stewards that include administering access to systems and data based on the documented authorizations. Effective access authorization practices include, among other things, the use of access authorization forms to document

[1] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[2] Department Topic No. 325-000-002, *Information Technology Resource User's Manual*, Chapter 2, *Access to the Department's Information Technology Resources*.

[3] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

the user access privileges authorized by management and to facilitate the complete and accurate assignment of user access privileges. Department procedures[4] require that the Automated Access Request Form (AARF) System be used to electronically document requests for access privileges and that the AARF requests be electronically approved by supervisors, cost center managers, and security coordinators within the AARF System.

To determine whether the FPM access privileges granted were authorized and appropriately assigned, we requested AARF System records for 10 of the 93 users with access privileges to the FPM as of October 26, 2016. Our examination disclosed that some AARF System records were missing or incomplete and, as a result, Department records did not demonstrate that the FPM access privileges granted were authorized by management. Specifically:

- Department management did not provide AARF System records for 2 of the 10 selected users.
- AARF System records provided for the other 8 users did not include the specific FPM access privileges requested.
    - For 6 of the 8 users, AARF System records did not include proper authorization by the supervisor and application owner as there was not a signature line for the FPM on the records for 5 users and the FPM signature line was blank on the record for the other user.

The maintenance of appropriately authorized, complete, and accurate access authorization records enhances management's ability to ensure and demonstrate that access privileges granted for users are appropriate for the users' assigned job duties.

Recommendation: We recommend that Department management improve controls to ensure that access privileges are only granted pursuant to properly completed and approved access authorization records and to require that such records be retained.

Finding 3: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and information technology (IT) resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Also, AST rules[5] require that each agency manage identities and credentials for authorized devices and users and ensure that IT access is removed when the IT resource is no longer required. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Our audit procedures disclosed some inappropriate and unnecessary access privileges to the FPM, the FM common database containing FPM data and tables, and the FPM production dataset containing FPM programs. Specifically:

- **FPM** – In connection with our examination of the AARF records discussed in Finding 2, Department management indicated that 2 of the 10 selected FPM users had inappropriate access privileges to the FPM. Also, the appropriateness of the access privileges was not supported by Department records for the 2 users discussed in Finding 2 for whom Department management did not provide us with the AARF System records.

[4] Department Topic No. 325-000-002, *Information Technology Resource User's Manual*, Chapter 2, *Access to the Department's Information Technology Resources*.

[5] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

- **FM Common Database Containing FPM Data and Tables** – We identified 91 user identification codes (user IDs) for users with certain table, database, and system access privileges to the FM common database containing the FPM data and tables as of October 4, 2016. Our examination of the access privileges for the 91 employees associated with these user IDs disclosed the existence of some inappropriate and unnecessary table and system access privileges to the database. Specifically, we found that:

  - Three employees had system access privileges to the database that were not appropriate for their job duties as database administrators and caused a separation of duties impairment.
  - Two employees had table access privileges to the database that were not appropriate for their job duties as end users. According to Department management, the two end users were not authorized to have FPM access and accordingly should not have FPM table access privileges.
  - Although 2 former employees had separated from Department employment, their active table access privileges to the database continued for 5 and 47 days, respectively, after their employment separation dates.

  Although we requested, Department management did not provide documentation supporting the appropriateness and necessity of the access privileges for 82 of the 91 user IDs. Also, Department management did not provide documentation evidencing that the access privileges for the 2 former employees were not used beyond the employees' separation dates. As a result, for these 82 user IDs and 2 former employees, the effectiveness of Department controls related to the appropriateness of access privileges to the database was not demonstrated.

- **FPM Production Dataset Containing FPM Programs** – We tested the access privileges of all 12 user IDs with access privileges to the FPM production dataset containing FPM programs as of October 26, 2016. Our audit procedures disclosed that 1 user ID belonged to an employee with inappropriate FPM production dataset access privileges and 1 user ID belonged to a former employee with active access privileges. Specifically, we found that:

  - A Department employee had inappropriate and unnecessary update access privileges to the FPM production dataset as the employee was improperly included as a member of an AST security group.
  - A former employee continued to have active access privileges for 1,916 days (over 5 years) after the employee's date of separation from Department employment.

  Although we requested, Department management did not provide documentation supporting the appropriateness and necessity of the access privileges for 9 of the 12 user IDs examined or evidence that the access privileges for the former employee were not used beyond the employee's separation date. As a result, for these 9 user IDs and the former employee, the effectiveness of the controls related to the appropriateness of access privileges to the FPM production dataset was not demonstrated.

The existence of inappropriate and unnecessary user access privileges to the FPM, the FM common database containing FPM data and tables, and the FPM production dataset increases the risk of unauthorized modification, loss, or disclosure of FPM data and related IT resources.

Recommendation: We recommend that Department management limit user access privileges to the FPM, the FM common database, and the FPM production dataset to restrict users to only those access privileges appropriate and necessary for the users' assigned job duties and timely deactivate user access privileges for former employees.

Finding 4: Separation of Duties

AST rules[6] require each agency to ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties. The Department uses a change management and automated production turnover system (change management system) that controls, moves, tracks, and provides an inventory of all FPM entries through the development lifecycle from test to production. Through user groups, the change management system allows for separation of duties for various activities. Specific user group membership defines the level of access privileges to those activities.

We selected the three Department user groups (Supervisor, Programmer, and Project Leader) within the change management system as of November 10, 2016, to determine whether membership in the groups provided for an appropriate separation of duties. Our audit procedures disclosed a separation of duties impairment related to Supervisor user group member access privileges. Specifically, we noted that the five members of the Supervisor user group could both add and approve move requests to have program changes implemented into the production environment. In addition, the five members of the Supervisor user group were also members of the Programmer and Project Leader user groups and the access privileges defined for the Programmer and Project Leader user groups also provided the capability in the change management system to add move requests.

Without effective controls in place to help ensure an appropriate separation of duties, the risk is increased that unauthorized program changes may be implemented into the production environment and not be timely detected.

Recommendation: We recommend that Department management implement controls to ensure that members of the Supervisor user group cannot add and approve move requests to implement program changes into the production environment.

Finding 5: Policies and Procedures – Access Controls

Effective IT controls include notifications to security management of employee separations from employment and the prompt deactivation of user IDs and passwords. Timely notification and prompt deactivation are necessary to ensure that the access privileges are not misused by former employees or others to compromise data or IT resources. Additionally, AST rules[7] require that control measures ensure that IT access is removed when the IT resource is no longer required.

We reviewed Department procedures to gain an understanding of the Department's directives for removing logical access privileges to IT resources, including the FPM. Our review disclosed that Department procedures defining the requirements for granting and removing access to the Department's IT resources need improvement. Specifically, Department procedures[8] require termination requests be submitted when an employee terminates his or her employment and that termination requests be processed by the Office of Information Technology Security, application owners notified, and access

[6] AST Rule 74-2.003(1)(d), Florida Administrative Code.

[7] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

[8] Department Topic No. 325-000-002, *Information Technology Resource User's Manual*, Chapter 2, *Access to the Department's Information Technology Resources.*

deactivated within 7 business days of the effective date of the termination request or upon receipt of the request, whichever is later. Allowing 7 business days or more before the deactivation of access privileges, rather than promptly deactivating the access privileges when no longer needed (e.g., within 1 to 2 business days of an employee's separation from employment), increases the risk that the access privileges may be misused to compromise FPM data or IT resources.

Recommendation: We recommend that Department management comply with AST rules and improve Department procedures to require that user access privileges be promptly deactivated when the access is no longer necessary.

Follow-Up to Management's Response

In the written response, Department management indicated concurrence with the finding and recommendation. However, management further stated that "the Department adheres to Florida Administrative Code which states that access will be removed promptly" and that "all termination requests shall be processed by OIT [Office of Information Technology] Security, application owners notified, and access revoked within seven (7) business days of the effective date as noted in [the] AARF [Automated Access Request Form] or upon receipt of the request, whichever is later." Notwithstanding this response, the point of our finding is that Department policy allowing 7 or more business days to elapse after an employee separates from Department employment before removing the employee's access privileges unnecessarily exposes the Department to an increased risk of loss or misuse of Department data or IT resources. Consequently, we continue to recommend that Department management comply with AST rules and improve Department procedures to require that user access privileges be promptly deactivated when the access is no longer necessary (e.g., within 1 to 2 business days of an employee's separation from employment).

Finding 6: Security Controls – User Authentication and Logging and Monitoring

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 FPM user authentication and logging and monitoring for FPM data and related IT resources need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FPM data and related 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. 2015-039 (finding No. 4).

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

Recommendation: We recommend that Department management improve certain security controls related to user authentication and logging and monitoring for FPM-related IT resources to ensure the continued confidentiality, integrity, and availability of FPM data and related IT resources.

PRIOR AUDIT FOLLOW-UP

As noted in Finding 6, Department management had not taken corrective actions to address finding No. 4 included in our report No. 2015-039.

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 September 2016 through November 2016 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to the Federal Programs Management subsystem (FPM) during the period July 2016 through November 2016. The audit included selected business process application controls over transaction data input, processing, output, and interfaces; selected application-level general controls over logical access and program changes for the FPM; and user authentication controls related to finding No. 4 disclosed in our report No. 2015-039. The overall objectives of the 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.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2015-039 that were applicable to the scope of this audit.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

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 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 this 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 the 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 the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This 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 this audit, we:

- Interviewed Department personnel and reviewed FPM-related documentation to obtain an understanding of:
  - The FPM data and business process flows, including key sources of data input, key application transactions and processes, key types of application data output, and interfaces and reconciliations related to the FPM.
  - The FPM computing platform including applicable hardware, operating system, database management system, and security software.
  - The user account management processes, including policies and procedures for authorizing, creating, modifying, and revoking FPM user and related IT resources accounts.
  - The program change management processes, including policies and procedures for application change control and the Department's system development life cycle methodology.
- Evaluated FPM business process application controls related to data input, processing, output, and interfaces. Specifically, we:
  - Evaluated the one data change request created on July 6, 2016, and related information to determine whether there were processes in place to ensure that data changes are authorized and do not produce erroneous data and to detect, report, and appropriately investigate data change request errors, should they occur.
  - Evaluated the adequacy of FPM input edit controls, as of October 11, 2016, to prevent the entry of erroneous data into the FPM. Specifically, we evaluated online edits for 15 key data fields related to the Federal Billing Control Financial Projects Update Event, Federal Billing Control Add Event, and the Federal Billing Control Agreement Maintenance Apply Event screens to determine whether the edits worked as intended by management to prevent erroneous data, including duplicate data, from being entered into the FPM.
  - Evaluated two job abended notifications, one dated August 31, 2016, and the other dated September 22, 2016, to determine whether controls were in place to ensure that data input from the Project Cost Management (PCM) subsystem is processed, with minimal intervention, by the FPM and that processing errors are identified and communicated to appropriate IT personnel.
  - Evaluated the *Reconciliation Report between FHWA and FM* for the Bill End Date of October 14, 2016, to determine whether reconciliation and monitoring controls were in place to identify, in advance, instances in which project reimbursement requests to be sent to the Federal Highway Administration (FHWA) Federal Management Information System (FMIS) exceed the Federal obligated amounts.
  - Evaluated a job abended notification dated September 22, 2016, to determine whether controls were in place to ensure that FPM transaction update jobs, or jobs that FPM depends on, are scheduled to run in a predetermined order to help reduce the risk of data corruption.

- Inspected documentation on October 11, 2016, and October 18, 2016, to determine whether controls were in place to prevent the processing of files multiple times (duplicate processing), to detect and prevent duplicate transactions, and to ensure reimbursement output files remain current.
- Inspected a weekly project listing report dated November 10, 2016, to determine whether a control was in place to ensure the accuracy of project coding (billing flag) and other project billing information.
- Observed on October 18, 2016, at the Department's Office of the Comptroller, and evaluated the process for creating and examining the report used to spot check the amounts in the reimbursement request for accuracy.
- Inspected the FHWA *FMIS 5.0 State Preparation Guide* to determine whether interface file procedures (upload and download) were in place related to the transmission of reimbursement requests.
- Inspected output on October 18, 2016, from the Automation Platform tool used to upload FMIS data to the Department's mainframe to determine whether a control was in place to identify interface file processing errors.

- Evaluated the FPM access controls for 10 of the 93 users with access privileges to the FPM as of October 26, 2016, to determine whether the FPM access privileges were authorized and appropriately assigned.
- Inspected security log information as of October 20, 2016, and related documentation to determine whether a control was in place to monitor the validity of new security accounts.
- Inspected Department procedures and inquired of Department management to determine whether access privileges were periodically reviewed to help ensure the continued appropriateness of the access privileges assigned.
- Inspected Department procedures and inquired of Department management to determine whether a control was in place to ensure the timely removal of access privileges for former employees.
- Inspected Department procedures and inquired of Department management to determine whether monitoring controls were in place to adequately protect certain information technology resources.
- Evaluated the effectiveness of access controls for the three Department user groups within the change management system as of November 10, 2016, to determine whether membership in the three groups provided for an appropriate separation of duties.
- Evaluated the access controls for all 91 user IDs of users with certain table, database, and system access privileges to the FM common database containing the FPM data and tables as of October 4, 2016, to determine whether the access privileges assigned were appropriate.
- Evaluated the effectiveness of access controls for all 12 user IDs with access privileges to the FPM production dataset containing FPM programs as of October 26, 2016, to determine whether the access privileges assigned were appropriate.
- Evaluated authentication controls for FPM and related IT resources.
- Inspected Department change management procedures and documentation and inquired of Department management to determine whether change management controls were in place to ensure that application changes were authorized, tested, approved, and appropriately implemented into production.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.

- Performed various other auditing procedures, including analytical 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 the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. 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.

Sherrill F. Norman, CPA
Auditor General

FDOT
Florida Department of Transportation
RICK SCOTT
GOVERNOR
605 Suwannee Street
Tallahassee, FL 32399-0450
RACHEL D. CONE
INTERIM SECRETARY

May 24, 2017

Sherrill F. Norman
Auditor General
Claude Denson Pepper Building
Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

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

Department of Transportation- IT Operational Audit
Federal Programs Management Subsystem (FPM)

As required by Section 11.45(4) (d), Florida Statutes, the department's responses and Corrective Action Plans for this IT operational audit 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,

Rachel D. Cone
Interim Secretary

RC: cm

Enclosure (1)

www.fdot.gov

Summary of Findings and Department Responses
Auditor General IT Operational Audit- FPM

Finding 1- Periodic Access Review: Department procedures did not provide for comprehensive and timely periodic reviews of application user access privileges and the Department had not performed a review of FPM user access privileges since May 2015 or reviews of other system access privileges since June 2013.

Recommendation: We recommend that Department management improve controls and enhance Department procedures to require the performance of periodic reviews of user access privileges granted for all Department applications. We also recommend that Department management ensure that annual recertifications of system user access privileges are performed as required by Department procedures.

Agency Response and Corrective Action Plan: We concur with the finding(s) and recommendation(s). The Department will ensure that periodic reviews of user access privileges for all Department applications is conducted. The Department will also ensure that an annual recertification of system user access privileges for the FPM system **will** be performed as required by Department procedure.

Estimated Corrective Action Date: June 30, 2018

Agency Contact and Telephone Number: Greg Smiley, Chief Information Officer, (850) 414-4771

Finding 2- Access Authorization Documentation: Department access controls need improvement to ensure that access granted is properly authorized and documented.

Recommendation: We recommend that Department management improve controls to ensure that access privileges are only granted pursuant to properly completed and approved access authorization records and to require that such records be retained.

Agency Response and Corrective Action Plan: We concur with the finding(s) and recommendation(s). The Department will modify the authorization request form to detail specific FPM authority and ensure these required authorization records are included with access requests prior to granting the requested access and that authorization records are retained within the Automated Access Request Form (AARF) system.

Estimated Corrective Action Date: May 1, 2018

Agency Contact and Telephone Number: Greg Smiley, Chief Information Officer, (850) 414-4771

Finding 3- Appropriateness of Access Privileges: The access privileges for some FPM, Financial Management common database, and FPM production dataset users did not restrict users to only those functions necessary for their assigned job duties.

Recommendation: We recommend that Department management limit user access privileges to the FPM, the FM common database, and the FPM production dataset to restrict users to only those access privileges appropriate and necessary for the users' assigned job duties and timely deactivate user access privileges for former employees.

Agency Response and Corrective Action Plan: We concur with the finding(s) and recommendation(s). The Department **will** ensure that access privileges for users **will** be appropriate

1

and necessary for the user's assigned job duties and that user access privileges **will** be deactivated timely when access is no longer required.

Estimated Corrective Action Date: May 1, 2018.

Agency Contact and Telephone Number: Greg Smiley, Chief Information Officer, (850) 414-4771

Finding 4- Separation of Duties: Some Department access controls related to the configuration management system need improvement to promote an appropriate separation of duties.

Recommendation: We recommend that Department management implement controls to ensure that members of the Supervisor user group cannot add and approve move requests to implement program changes into the production environment.

Agency Response and Corrective Action Plan: We concur with the finding(s) and recommendation(s). The Department will ensure that no user can both add and approve move requests to implement program changes into the production environment.

Estimated Corrective Action Date: July 1, 2018

Agency Contact and Telephone Number: Greg Smiley, Chief Information Officer, (850) 414-4771

Finding 5- Policies and Procedures- Access Controls: Department procedures defining the requirements for obtaining and removing access to the Department's IT resources need improvement.

Recommendation: We recommend that Department management comply with AST rules and improve Department procedures to require that user access privileges be promptly deactivated when the access is no longer necessary.

Agency Response and Corrective Action Plan: We concur with the finding(s) and recommendation(s). The Department adheres to Florida Administrative Code which states that access will be removed timely. Department policy states that all termination requests shall be initiated by the user's business unit and approved by the Cost Center Manager in the Automated Access Request Form (AARF) no later than the user's separation date. All termination requests shall be processed by OIT Security, application owners notified, and access revoked within seven (7) business days of the effective date as noted in AARF or upon receipt of the request, whichever is later.

Estimated Corrective Action Date: N/A

Agency Contact and Telephone Number: Greg Smiley, Chief Information Officer, (850) 414-4771

Finding 6- Security Controls- User Authentication and Logging and Monitoring: Certain Department security controls related to FPM user authentication and logging and monitoring for FPM data and related IT resources need improvement.

Recommendation: We recommend that Department management improve certain security controls related to user authentication and logging and monitoring for FPM-related IT resources to ensure the continued confidentiality, integrity, and availability of FPM data and related IT resources.

Agency Response and Corrective Action Plan: We concur with the finding(s) and recommendation(s). Changing certain security controls would require resources that are currently not

available vs. operational requirements. Additionally, the FM system, of which FPM is a sub-system, is due to be replaced in the relatively near future, which will engage resources as well as require extensive re-writing of subsystems. In light of all the aforementioned factors, management assumes the inferred risk.

In regard to Logging and Monitoring, we concur with the finding(s) and recommendation(s). Management will review the feasibility of enabling more intensive monitoring.

Estimated Corrective Action Date: June 30, 2018

Agency Contact and Telephone Number: Greg Smiley, Chief Information Officer, (850) 414-4771

3