Six-Month Update
Auditor General IT Operational Audit of Department of Transportation- Federal Programs Management Subsystem (FPM)
Report 2017-206

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.
>
> **Six Month Follow-Up Response:** Complete.
>
> **Estimated Completion Date:** N/A

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.
>
> **Six Month Follow-Up Response:** Complete.
>
> **Estimated Completion Date:** N/A

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

Six Month Follow-Up Response: Complete.

Estimated Completion Date: N/A

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 Completion Date: Complete.

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 Completion Date: Complete.

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.

Six-Month Update
Auditor General IT Operational Audit of Department of Transportation- Federal Programs Management Subsystem (FPM)
Report 2017-206

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.

Six Month Follow-Up Response: The rewrite of FPM falls within the scope of the Work Program Integration Initiative project, which is estimated to be completed June 30, 2021. FPM access authorization utilizes multiple layers of security including FDOT access, AARF approval, RACF Id and RACF Group as well as FM Gen Security to prevent unauthorized use of FPM. Management will review the feasibility of enabling more intensive monitoring during the rewrite.

Estimated Completion Date: June 30, 2018