Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

A SAFER
FLORIDA
HIGHWAY SAFETY AND MOTOR VEHICLES

April 9, 2018

Ms. Terry L. Rhodes
Executive Director
Department of Highway Safety and Motor Vehicles
2900 Apalachee Parkway B443
Tallahassee, Florida 32399-0500

Re: Auditor General Report No. 2018-022
Department of Highway Safety Information Technology Operational Audit - Florida Real Time Information System

Dear Ms. Rhodes:

In accordance with Section 20.055(6)(h), Florida Statutes, we are providing an assessment of the implementation or current status of the recommendations in the Auditor General's Report No. 2017-088.

If you need additional information, please contact me at 617-3104.

Sincerely,

Julie M. Leftheris
Inspector General

cc: Ms. Kathy Dubose, Coordinator, Joint Legislative Auditing Committee

Source of Audit: Auditor General
Report Number: 2018-022
Report Title: Department of Highway Safety Operational Report

Finding No. 1: Appropriateness of Access Privileges

Some Department employee, contractor, and outside agency employee access privileges to the FRVIS; the FRVIS database, database developer roles; or program source code, parameters, or data libraries did not promote an appropriate separation of duties or did not appropriately restrict the users' access to only those functions necessary for their assigned job duties. Also, the Department did not timely deactivate access privileges when the access was no longer necessary.

Recommendation: We recommend that Department management limit user access privileges to FRVIS; the FRVIS database; database developer roles; and program source code, parameters, and data libraries to promote an appropriate separation of duties and restrict users to only those access privileges necessary for the users' assigned job duties. Department management should also ensure that access privileges are timely deactivated when the access is no longer necessary.

Initial Response: As noted during our exit conference the Department has made significant strides in improving controls related to the legacy FRVIS system. We appreciate your input and the Department's procedures will be enhanced to further limit user access privileges to promote appropriate segregation of duties and restrict users to only those access privileges that are necessary for their Department assigned job duties. In order to accomplish this enhancement, all FRVIS user roles were reviewed with the user's respective supervisors. Any roles that were determined to be unnecessary due to changes in Department procedures were removed. Although the use of network access software prevented terminated users from accessing Department systems and databases, the Department implemented secondary control procedures in April 2017 to ensure that User IDs are also terminated at the same time as their network access. All former employees, contractor's and Agent's User Ids will be deactivated upon notice of termination. All batch jobs with associated User IDs have been reviewed and obsolete batch jobs User IDs have been deactivated. Additionally, beginning in January 2018, new database auditing and logging features that are available after our 2017 upgrade will be utilized to further mitigate risk until this legacy system is replaced.

Six month Response: The Information Services Administration implemented new reporting processes related to inactive accounts to ensure access is removed for Active Directory, FRVIS, and the Oracle databases. Information Services Administration also deactivated inactive FRVIS and Oracle databases accounts, deleted unnecessary user roles, and removed unnecessary access for users with access to program source code, parameters, or data libraries.

Status: Closed

Finding No. 2: Retention of Access Control Records

Contrary to the State of Florida *General Records Schedule GS1-SL for State and Local Government Agencies*, the Department did not retain relevant FRVIS access control records related to the deactivation of employee access privileges.

Recommendation: We recommend that Department management ensure that relevant access control records related to the FRVIS database are retained as required by the General Records Schedule.

Agency Response: Effective January 1, 2018, the Department will move from a manual tracking process to an electronic process that captures all requests for access privileges including onboarding, changing job duties and offboarding. Maintaining these records electronically in a single location will ensure compliance with the General Records Schedule.

Six month Response: The Information Systems Administration implemented onboarding, offboarding, and transfer processes to ensure access is appropriately issued, maintained, or removed.

Status: Closed

Finding No. 3: Continuity of Operations

The Department did not perform quarterly testing or an annual audit of the Division of Information Systems Administration's Continuity of Operations Plan.

Recommendation: We recommend that Department management conduct quarterly testing and annual audits as specified in the COOP to ensure the recoverability of Department operations in the event of a disaster or other interruption of service.

Agency Response: The Department's various Division COOPs were updated and consolidated in 2017 in cooperation with the Division of Emergency Management. Information Systems Administration leadership will complete COOP testing in accordance with the requirements of the new Department COOP.

Six month Response: The Information Systems administration updated its COOP plan in accordance with the updated Department COOP, and is in the process of developing testing based on the requirements set forth in the updated COOP plan.

Status: Open

Finding No. 4: Security Controls – User Authentication and Logging and Monitoring

Certain security controls related to user authentication and logging and monitoring for FRVIS data and related IT resources need improvement to ensure the confidentiality, integrity, and availability of FRVIS data and related IT resources.

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

Agency Response: The Department has made significant strides to improve the security controls related to user authentication. Due to the implementation of the new version of our database management system and enterprise hardware, the Department will be able to further enhance the security controls on this legacy system to make the suggested improvements in user authentication, logging and monitoring. These improvements will ensure the confidentiality, integrity and availability of FRVIS data and related IT resources. Additionally, the Department's implementation of a managed security service will further mitigate risk to Department systems.

Six month Response: The Information Systems Administration improved certain security controls for FRVIS related to user authentication, logging, and monitoring changes.

Status: Closed