

**DEPARTMENT OF HIGHWAY SAFETY
AND MOTOR VEHICLES**

**FLORIDA REAL TIME VEHICLE INFORMATION
SYSTEM (FRVIS)**

Information Technology Operational Audit



EXECUTIVE DIRECTOR OF THE DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES

Pursuant to Section 20.24(1), Florida Statutes, the head of the Department of Highway Safety and Motor Vehicles is the Governor and Cabinet, which consists of the Attorney General, Chief Financial Officer, and Commissioner of Agriculture. Pursuant to Section 20.05(1)(g), Florida Statutes, the Governor and Cabinet are responsible for appointing the Executive Director of the Department of Highway Safety and Motor Vehicles. Julie L. Jones served as the Executive Director during the period of our audit.

The audit team leader was Art Wahl, CPA, CISA, 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 HIGHWAY SAFETY AND MOTOR VEHICLES

Florida Real Time Vehicle Information System (FRVIS)

SUMMARY

The Department of Highway Safety and Motor Vehicles (Department) maintains the Florida Real Time Vehicle Information System (FRVIS) that facilitates the collection of taxes and fees for tags, titles, and registrations associated with motor vehicles and vessels.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to FRVIS input, processing, and output. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2008-188.

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

Finding No. 1: Department data-entry procedures to ensure that all source documents applicable to FRVIS transactions are scanned into FRVIS needed improvement.

Finding No. 2: As similarly noted in our report No. 2008-188, some Department employees, contractors, and outside agency employees had inappropriate access to FRVIS as well as FRVIS programs and the FRVIS database that was unnecessary for their assigned job duties and did not enforce an appropriate separation of duties.

Finding No. 3: The Department did not timely deactivate access privileges of some former employees.

Finding No. 4: The Department had not performed periodic reviews of user access privileges to FRVIS and the FRVIS database.

Finding No. 5: Contrary to the State of Florida *General Records Schedule GS1-SL* retention requirements, the Department did not retain relevant FRVIS access control records related to the deactivation of employee access privileges.

Finding No. 6: As similarly noted in our report No. 2008-188, certain security controls related to FRVIS user authentication and session controls needed improvement.

Finding No. 7: As similarly noted in our report No. 2008-188, certain IT controls related to the monitoring of FRVIS database changes needed improvement.

Finding No. 8: Department procedures for verification of program changes made to the FRVIS production environment needed improvement.

Finding No. 9: Department change control procedures for FRVIS were not fully documented.

BACKGROUND

The Department of Highway Safety and Motor Vehicles, Division of Motorist Services, is responsible for tags, titles, and registrations for motor vehicles and vessels. Information Systems Administration (ISA) is responsible for meeting the information technology needs of the Department and maintaining FRVIS. Section 320.02(1), Florida Statutes, requires, except as otherwise provided by law, that motor vehicles operated or driven on the roads of Florida shall be registered in the State. Chapter 320, Florida Statutes, specifies various taxes and fees that shall be charged in connection with the registration of a motor vehicle. Chapter 328, Florida Statutes, addresses registration fees associated with vessels.

FRVIS is the application maintained by the Department to issue and account for tags, titles, and registrations for motor vehicles and vessels. Local tax collector and tag agent offices throughout the State process tag, title, and

registration transactions through FRVIS. According to the Department, FRVIS processed approximately 335 million transactions for the collection of approximately \$2.3 billion in revenue from taxes and fees associated with tags, titles, and registrations for motor vehicles and vessels during the 2012-13 fiscal year, including amounts retained by local tax collector and tag agent offices. These funds, together with all other sources of the Department's revenue, are distributed through FRVIS to various State agencies, including the Department, and non-State entities in accordance with governing Florida Statutes. During the 2012-13 fiscal year, approximately 347 million transactions from all revenue sources were processed through FRVIS for distributions of approximately \$2.8 billion, including the amounts retained by local agencies.

FRVIS is composed of two processing environments. The first is a distributed environment that consists of the servers at local tax collector and tag agent offices that process tag, title, and registration transactions throughout the State. The second environment is the host portion that consists of the back-end processing that is conducted centrally at the Department's primary data center.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Data-Entry Procedures

Effective data-entry procedures ensure that source documentation, input file data collection, and input preparation and entry are effectively controlled and that data is complete and accurate. Transactions are entered into FRVIS at local tax collector and tag agent offices throughout the State. Supporting documentation applicable to FRVIS transactions at each of the respective offices is sent to the Department for batching and scanning into FRVIS. Once the supporting documentation is scanned by Department staff, it is shredded.

As part of the Department's batching and scanning process, controls in FRVIS identified all transactions that were lacking scanned copies of the supporting documentation. Reports were generated by FRVIS disclosing the transactions for which supporting documentation had not but should have been scanned. Department staff stated that they used these reports to attempt to locate the missing supporting documentation including follow-ups with applicable tax collector or tag agent offices, if necessary. However, once efforts to locate the missing supporting documentation were performed and the documentation had not been located, there were no additional procedures to track or aggregately report to Department management on the missing supporting documentation to ensure appropriate action was taken. Without an appropriate procedure in place to track and aggregately report missing FRVIS supporting documentation, there is an increased risk that appropriate action may not be taken to ensure FRVIS transactions are complete and accurate.

Recommendation: The Department should implement a procedure to track and aggregately report on missing supporting documentation that was not scanned into FRVIS to help ensure the completeness and accuracy of FRVIS transactions.

Finding No. 2: Appropriateness of Access Privileges

Effective access controls include measures that limit employee, contractor, and outside agency employee access privileges to only what is necessary in the performance of assigned job duties and enforce an appropriate separation of duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Agency for Enterprise Information Technology (AEIT)¹ Rule 71A-1.007(5), Florida Administrative Code, provides that, for functions susceptible to fraudulent or other unauthorized activity, the agency shall ensure separation of duties so no individual has the ability to control the entire process. AEIT Rule 71A-1.007(3), Florida Administrative Code, provides that workers shall be authorized access to agency IT resources based on the principles of “least privilege” (the principle that grants the minimum possible privileges to permit a legitimate action) and “need to know” (the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties).

Our review of the appropriateness of access privileges to FRVIS; production source code, parameter, Job Control Language (JCL), and data libraries; and the FRVIS database disclosed that some users, including employees, contractors, and outside agency employees, had update access privileges that were not necessary for their job duties and did not enforce an appropriate separation of duties. These conditions increase the risk of errors, fraud, misuse, or other unauthorized modification of FRVIS data. Specifically:

- As similarly noted in our report No. 2008-188, one Department employee had inappropriate access privileges to the FRVIS production source code, parameter, JCL, and data libraries because of a lack of separation of incompatible security administration and programming duties.
- Access granted to FRVIS required the access privileges to be assigned through FRVIS as well as through the FRVIS database. The FRVIS database access privileges can be restricted to allow active access to the database only when the user accesses it through FRVIS. This forces the users’ access privileges to be subject to FRVIS edits and controls. However, we noted numerous instances where FRVIS database access privileges were not restricted from directly accessing the database increasing the opportunity for a user to bypass FRVIS edits and controls. The Department had not reviewed FRVIS database access privileges to ensure that the users were properly restricted from directly accessing the database.
- Our review of 60 FRVIS database user identification codes (IDs) that were also used to control access within FRVIS indicated the following:
 - One user ID assigned to a field tax collector’s office employee (outside agency employee) had been assigned FRVIS access privileges that were designated for Department use only.
 - One user ID assigned to a Department employee was still active in FRVIS and the FRVIS database for more than 5 ½ years after the employee’s termination of employment.
 - Seventeen user IDs assigned to field tax collectors’ office employees (outside agency employees) and Department employees that had their access privileges within FRVIS deactivated still had active access privileges within the FRVIS database. This included one user ID assigned to a former Department employee that remained active in FRVIS for more than seven months after the employee’s termination of employment.

The access privileges of the two former Department employees described above were not used subsequent to their employment terminations. Absent the removal of these access privileges within the database, 67 Department employees had the ability to reactivate these FRVIS privileges. Of the 67 Department employees, 29 could only reactivate these privileges through a direct database connection.

- As similarly noted in our report No. 2008-188, our review of FRVIS database access privileges identified the following:
 - Twenty-nine user IDs of 27 Department development employees and contractors with inappropriate access privileges that would allow them the capability to alter database tables that were critical to fee calculations in FRVIS.

¹ During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

- Eleven user IDs of Department employees who were not developers with inappropriate access privileges that would allow them the capability to alter database tables that were critical to fee calculations in FRVIS.
- Fifteen user IDs of 14 former Department employees with the inappropriate access privileges described above who had terminated employment between 6 and 45 months prior to our audit.
- Twenty-three user IDs with the inappropriate access privileges described above where the Department had not identified the user originally assigned to the user ID.

For the 14 former Department employees, the Department did not determine if the access privileges had been used after termination of employment.

Recommendation: The Department should ensure that the access privileges of employees, contractors, and outside agency employees are commensurate with their job duties and enforce an appropriate separation of duties.

Finding No. 3: Timely Deactivation of Access Privileges

Effective IT access controls include provisions for the timely deactivation of former employee access privileges to ensure that access privileges are not misused by the former employee. However, as previously identified in Finding No. 2, the access privileges of some former employees had not been deactivated in a timely manner. Without the timely deactivation of former Department employee access privileges, the risk was increased that the access privileges may be misused by the former employees or others.

Recommendation: The Department should ensure that access privileges of former employees are timely deactivated to minimize the risk of compromising FRVIS data and IT resources.

Finding No. 4: Periodic Review of Access Privileges

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 individuals have access and that the access provided to each user remains appropriate. As indicated by the excessive access privileges noted in Finding No. 2 above, the lack of periodic reviews of access privileges to FRVIS and the FRVIS database increases the risk that inappropriate access privileges may not be timely detected or remediated and may result in unauthorized or inappropriate changes to FRVIS data and programs.

Recommendation: The Department should perform periodic reviews of user access privileges to FRVIS and the FRVIS database to ensure that user and system account access privileges are authorized and remain appropriate.

Finding No. 5: Retention of Access Control Records

State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule)* provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. Contrary to the requirements of the *General Records Schedule*, the Department did not retain relevant FRVIS access control records related to the deactivation of employee access privileges. Without adequate retention

of relevant FRVIS access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur.

Recommendation: The Department should ensure that relevant FRVIS access control records are retained as required by the *General Records Schedule*.

Finding No. 6: User Authentication and Session Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls related to FRVIS in the areas of user authentication and session controls that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management and staff of the specific issues. Some of the issues were communicated to Department management in connection with our report No. 2008-188. Without adequate security controls related to certain user authentication and session controls, the confidentiality, integrity, and availability of FRVIS data and IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to certain user authentication and session controls to ensure the continued confidentiality, integrity, and availability of FRVIS data and IT resources.

Finding No. 7: Monitoring of FRVIS Database Changes

IT monitoring controls are intended to ensure the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain IT controls related to the monitoring of FRVIS database changes that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FRVIS data and IT resources. However, we have notified appropriate Department management and staff of the specific issues. This issue was also communicated to Department management in connection with our report No. 2008-188. Without adequate security controls related to monitoring of certain FRVIS database changes, the confidentiality, integrity, and availability of FRVIS data and IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to monitoring of database changes to ensure the continued confidentiality, integrity, and availability of FRVIS data and IT resources.

Finding No. 8: Program Changes to the FRVIS Production Environment

Effective controls over modification of application programs help ensure that only approved program changes are implemented. The effectiveness of ensuring that only approved program changes are implemented is enhanced when automated reports or system logs of program changes are generated and reviewed.

The Department did not have a mechanism in place to ensure that all program changes made to the FRVIS production environment were properly approved. Without a process for verifying that all program changes that occur in the FRVIS production environment are approved program changes that have gone through the appropriate program change control procedures, the risk is increased that erroneous or unauthorized program changes, should they be moved into the production environment, will not be timely detected by management.

Recommendation: The Department should implement a mechanism to ensure that all program changes made to the FRVIS production environment are properly approved.

Finding No. 9: Program Change Management Procedures

Effective controls over the modification of application programs help ensure that only authorized, tested, and approved changes are implemented. The effectiveness of program change controls is enhanced when management's expectations for the control of program changes are documented in the form of written procedures.

The Department had documented some of the procedures being used to manage changes to FRVIS programs. However, key components of the project life cycle and methodology were incomplete such as end-user input, testing, and approvals. Also, procedures did not identify the staff responsible for development, programming, testing, and implementation. Without documentation of management's expectations for the control of program changes, the risk is increased that erroneous or unauthorized program changes could be moved into the production environment.

Recommendation: The Department should enhance program change management procedures to include end-user input, testing, and approvals throughout all phases of the change management process. Also, the Department's procedures should identify staff responsible for development, programming, testing, and implementation.

PRIOR AUDIT FOLLOW-UP

Except as noted in the preceding paragraphs, for those audit findings disclosed in our report No. 2008-188 that continued to be relevant and were within the scope of this audit, the Department had taken corrective actions.

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 2013 through January 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, audit findings disclosed in audit report No. 2008-188 that were within the scope of this audit.

The scope of our audit focused on evaluating selected application input, processing, and output controls applicable to FRVIS during the period July 2013 through January 2014 and selected Department actions through February 28, 2014. The audit included selected general IT controls over system modification and logical access to programs and data.

This audit was designed to identify, for the IT systems 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 systems 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 systems 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 FRVIS, including the purpose, goals, and background information involving financial, operation, and compliance requirements; the network computing platform and user duties; the logical access procedures used for granting access privileges to FRVIS, the FRVIS database, and the network; the identification and protection of confidential and exempt FRVIS information; and the Department's change management process applicable to FRVIS.
- Observed and evaluated the effectiveness of selected FRVIS input, processing, and output controls, as well as exception reporting, correcting, modifying, logging, and follow-up procedures, in promoting data integrity, completeness, and accuracy.
- Evaluated the effectiveness of selected controls over the authorization, documentation, testing, approval, and implementation of six FRVIS program changes completed between July 1, 2013, and October 18, 2013.
- Evaluated the effectiveness of selected logical access controls, including password and logging settings, in ensuring that access privileges to the Department's network, FRVIS, FRVIS servers, and the FRVIS database were appropriately restricted and provided an adequate separation of duties.
- Evaluated the effectiveness of selected logical access controls for the FRVIS mainframe JCL, programs, data files, and other datasets in ensuring that access privileges were appropriately restricted and provided an adequate separation of duties.
- Observed and evaluated the Department's compliance with State law for selected taxes and fees related to FRVIS.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

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 April 3, 2014, the Executive Director 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

Julie L. Jones
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0600
www.flhsmv.gov



Rick Scott
Governor

Pam Bondi
Attorney General

Jeff Atwater
Chief Financial Officer

Adam Putnam
Commissioner of Agriculture

April 3, 2014

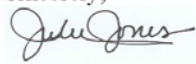
David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Thank you for the opportunity to respond to the preliminary and tentative findings and recommendations from your information technology operational audit of the Department of Highway Safety and Motor Vehicles' Florida Real Time Vehicle Information System (FRVIS). We appreciate the efforts of your staff and in accordance with Section 11.45(4)(d), Florida Statutes, we have included our response to the recommendations made in your report.

The Department of Highway Safety and Motor Vehicles is committed to providing highway safety and security through excellence in service, education, and enforcement. The results of your report will be used as part of the Department's continuous efforts to improve operations.

If you have any questions regarding our response, please contact David Ulewicz, Audit Director, at (850) 617-3104.

Sincerely,

Julie L. Jones
Executive Director

JLJ/jl
Enclosure

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Highway Safety and Motor Vehicles
Response to the Auditor General's Operational Audit
Of the Department of Highway Safety and Motor Vehicles'
Florida Real Time Vehicle Information System (FRVIS)
Preliminary and Tentative Audit Findings

Finding No. 1: Data-Entry Procedures

Department data-entry procedures to ensure that all source documents applicable to FRVIS transactions are scanned into FRVIS needed improvement.

Recommendation

The Department should implement a procedure to track and aggregately report on missing supporting documentation that was not scanned into FRVIS to help ensure that the completeness and accuracy of FRVIS transactions.

Agency Response

The Department will develop and implement a procedure to improve the identifying and tracking of missing support documentation for FRVIS transactions. This will include notifying agencies that are not in compliance with policies and procedures regarding the reporting of title transactions. The reengineering of the FRVIS application is included in the Department's Motorist Modernization project and additional process improvements to enhance the auditing and tracking of documents will be addressed as a part of this effort.

Finding No. 2: Appropriateness of Access Privileges

As similarly noted in our report No. 2008-188, some Department employees, contractors, and outside agency employees had inappropriate access to FRVIS as well as FRVIS programs and the FRVIS database that was unnecessary for their assigned job duties and did not enforce an appropriate separation of duties.

Recommendation

The Department should ensure that the access privileges of employees, contractors, and outside agency employees are commensurate with their job duties and enforce an appropriate separation of duties.

Agency Response

The Motorist Services FRVIS Access Authorization Request form will be reviewed upon receipt to determine that the requested roles are needed to perform job duties. Documentation will be retained.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Highway Safety and Motor Vehicles
Response to the Auditor General's Operational Audit
Of the Department of Highway Safety and Motor Vehicles'
Florida Real Time Vehicle Information System (FRVIS)
Preliminary and Tentative Audit Findings

Finding No. 3: Timely Deactivation of Access Privileges

The Department did not timely deactivate access privileges of some former employees.

Recommendation

The Department should ensure that access privileges of former employees are timely deactivated to minimize the risk of compromising FRVIS data and IT resources.

Agency Response

The Department updated Motorist Services procedures TL-57 and RS-64 effective January 1, 2014 to routinely suspend and/or delete any FRVIS user that has not accessed the FRVIS System in 90 days. In addition, the Department has reviewed and identified FRVIS user accounts that will be deleted and/or disabled.

Finding No. 4: Periodic Review of Access Privileges

The Department had not performed periodic reviews of user access privileges to FRVIS and the FRVIS database.

Recommendation

The Department should perform periodic reviews of user access privileges to FRVIS and the FRVIS database to ensure that user and system account access privileges are authorized and remain appropriate.

Agency Response

The Department will perform a periodic review of user access privileges to FRVIS by providing a list of users and roles for verification to tax collector/agents and department managers.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Highway Safety and Motor Vehicles
Response to the Auditor General's Operational Audit
Of the Department of Highway Safety and Motor Vehicles'
Florida Real Time Vehicle Information System (FRVIS)
Preliminary and Tentative Audit Findings

Finding No. 5: Retention of Access Control Records

Contrary to the State of Florida General Records Schedule GS1-SL retention requirements, the Department did not retain relevant FRVIS access control records related to the deactivation of employee access privileges.

Recommendation

The Department should ensure that relevant FRVIS access control records are retained as required by the General Records Schedule.

Agency Response

Motorist Services Support procedures require the retention of a copy of the FRVIS Access Authorization Request for all new users, change requests, and delete requests as required by the General Records Schedule. As indicated above, the Department did not timely deactivate all former employees and did not retain the associated documentation related to all of the deactivations. In our response to Audit Finding No. 3, the Department updated our procedures to address the timely deactivation of access privileges of former employees and will retain any reports and/or a copy of the FRVIS Access Authorization Requests used to delete access privileges of former employees as required by the General Records Schedule.

Finding No. 6: User Authentication and Session Controls

As similarly noted in our report No. 2008-188, certain security controls related to FRVIS user authentication and session controls needed improvement.

Recommendation

The Department should implement appropriate security controls related to certain user authentication and session controls to ensure the continued confidentiality, integrity, and availability of FRVIS data and IT resources.

Agency Response

The Department has begun research and documentation to determine impact and risk to the environment based upon any required changes. Upon completion of the risk assessment, the Department will implement enhanced security controls to address the audit recommendation. The Department has identified administrative features within Oracle that provide more granular security attributes. Documentation of the findings and a preliminary plan addressing required changes is being developed.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

**Department of Highway Safety and Motor Vehicles
Response to the Auditor General's Operational Audit
Of the Department of Highway Safety and Motor Vehicles'
Florida Real Time Vehicle Information System (FRVIS)
Preliminary and Tentative Audit Findings**

Finding No. 7: Monitoring of FRVIS Database Changes

As similarly noted in our report No. 2008-188, certain IT controls related to the monitoring of FRVIS database changes needed improvement.

Recommendation

The Department should implement appropriate security controls related to monitoring of database changes to ensure the continued confidentiality, integrity, and availability of FRVIS data and IT resources.

Agency Response

As mentioned in Audit Finding No. 6, the Department has identified administrative features within Oracle that provide more granular security attributes. The Department will review their application and database security controls and develop a comprehensive plan to improve security controls. The plan shall be completed within 6 months.

Finding No. 8: Program Changes to the FRVIS Production Environment

Department procedures for verification of program changes made to the FRVIS production environment needed improvement.

Recommendation

The Department should implement a mechanism to ensure that all program changes made to the FRVIS production environment are properly approved.

Agency Response

The Department's change management function has established policy, process and procedures, and Change Advisory and Technical Review governance boards to ensure that all changes made to the production environment are recorded, assessed for risk and impact and released in a controlled manner. We have implemented an industry best practice toolset.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Highway Safety and Motor Vehicles
Response to the Auditor General's Operational Audit
Of the Department of Highway Safety and Motor Vehicles'
Florida Real Time Vehicle Information System (FRVIS)
Preliminary and Tentative Audit Findings

Finding No. 9: Program Change Management Procedures

Department change control procedures for FRVIS were not fully documented.

Recommendation

The Department should enhance program change management procedures to include end-user input, testing, and approvals throughout all phases of the change management process. Also, the Department's procedures should identify staff responsible for development, programming, testing, and implementation.

Agency Response

As mentioned in Audit Finding No. 8, the Department has a change management function supported by a governance process that authorizes projects which require program changes. In addition, the Department's service request system confirms priority on programming tasks, followed by the Department's change management procedures which are fully documented with Technical Review and Change Advisory Boards. Change management receives the output of the User Acceptance Testing (UAT) outlining the authorization given by the business to release the change. A component of the required information for change submission is to identify, test, and back-out plans for both test and production environments. In order for an implementation to be closed, the implementer must provide closure comments as to the success or issues experienced with the change. The change management process then validates through Post Implementation Review (PIR), the overall success or failure of the change. The criteria for PIR completion is outlined in the Change Management Policy Document and is now part of the project closure process.