STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-022
October 2017

DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES

Florida Real Time Vehicle Information System

Sherrill F. Norman, CPA
Auditor General

Executive Director of the Department of Highway Safety and Motor Vehicles

The Department of Highway Safety and Motor Vehicles is established by Section 20.24, Florida Statutes. The head of the Department is the Governor and Cabinet. Pursuant to Section 20.05(1)(g), Florida Statutes, the Governor and Cabinet are responsible for appointing an Executive Director of the Department. Terry L. Rhodes served as Executive Director during the period of our audit.

The team leader was Wayne Revell, 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 are available at:

FLAuditor.gov

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 HIGHWAY SAFETY AND MOTOR VEHICLES

Florida Real Time Vehicle Information System

SUMMARY

This operational audit of the Department of Highway Safety and Motor Vehicles (Department) focused on evaluating selected information technology (IT) controls applicable to the Florida Real Time Vehicle Information System (FRVIS) and included a follow-up on the findings noted in our report No. 2014-183. Our audit disclosed the following:

Finding 1: Some Department employee, contractor, and outside agency employee access privileges to 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.

Finding 2: 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.

Finding 3: The Department did not perform quarterly testing or an annual audit of the Division of Information Systems Administration's *Continuity of Operations Plan*.

Finding 4: 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.

BACKGROUND

State law[1] requires, except as otherwise provided by law, that motor vehicles operated or driven on roads in Florida be registered in the State and specifies various fees and taxes that must be charged in connection with the registration of a motor vehicle, mobile home, or vessel. The Department of Highway Safety and Motor Vehicles (Department), Division of Motorist Services, is responsible for motor vehicle, mobile home, and vessel tags, titles, and registrations and the Department maintains the Florida Real Time Vehicle Information System (FRVIS) to facilitate the collection of fees and taxes associated with the tags, titles, and registrations.

County tax collector and tag agent offices throughout the State process tag, title, and registration transactions through FRVIS. The funds associated with these transactions, together with all other sources of the Department's revenues, are distributed through FRVIS to various State agencies, including the Department, and non-State entities in accordance with State law.[2] According to Department records,

[1] Section 320.02(1), Chapter 320, and Chapter 328, Florida Statutes.

[2] Chapters 207, 319, 320, 322, and 328, Florida Statutes.

during the 2015-16 fiscal year, 383 million transactions totaling $2.75 billion, including 365 million tag, title, and registration transactions totaling $2.08 billion, were processed through FRVIS.

FRVIS is composed of two processing environments. The first is a distributed environment that consists of the servers at 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 State Data Center.

FINDINGS AND RECOMMENDATIONS

Finding 1: 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, Agency for State Technology (AST) rules[3] require that each agency manage the 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 FRVIS; the FRVIS database; database developer role; or program source code, parameters, or data libraries. Specifically:

- Our review of the FRVIS access privileges granted to 60 users (Department employees and outside agency employees), selected from the 5,287 users with access to the FRVIS roles that allowed update to Department screens and the tax collectors' office screens within FRVIS as of April 11, 2017, disclosed that:
  - Access privileges granted to 4 of the 60 users were inappropriate based on the users' job duties.
  - Access privileges granted to 1 of the 60 users, a former Department employee, were active in FRVIS and the FRVIS database for 1,411 days after the employee's separation date.
- We identified 41 user identification codes (user IDs) for which FRVIS database access privileges as of February 17, 2017, were not restricted from directly accessing the database. We selected 9 of the 41 user IDs for further evaluation and determined that the access granted to 8 of the 9 user IDs was inappropriate. Specifically, we found that:
  - Although the FRVIS access privileges had been deactivated for 2 user IDs assigned to former Department employees, the user IDs remained active in the FRVIS database for 624 and 1,785 days, respectively, after the employees' dates of separation from Department employment. Department management could not determine if the access privileges were used after the employees' separation dates.
  - 4 of the user IDs assigned to Department employees were granted access privileges that were inappropriate for the users' job duties.
  - 2 of the user IDs assigned to batch jobs were no longer being used.

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

- Our review of the 75 user IDs assigned a database developer role that, as of February 17, 2017, allowed update object access privileges disclosed inappropriate access privileges. Specifically, we found that:
  - 21 user IDs assigned to Department employee and contractor developers had inappropriate access privileges that allowed them the capability to alter FRVIS database tables that were critical to fee calculations in FRVIS.
  - 8 user IDs assigned to Department employees who were not developers had inappropriate access privileges that allowed them the capability to alter FRVIS database tables that were critical to fee calculations in FRVIS.
  - 22 user IDs assigned to 21 former Department employees and contractors remained active from 340 to 6,700 days after their employment separation or contract termination dates. In addition, Department management was unable to provide a separation date for 1 former user. In response to our inquiry, Department management stated on May 9, 2017, that 13 user IDs assigned to former Department employees and a contractor had been deactivated. The Department could not determine if the access privileges were used beyond the 21 employees' separation and contractors' termination dates.
  - Department management was unable to provide the identity of the users assigned 22 user IDs. Therefore, we were unable to determine whether the access privileges granted for these 22 user IDs were appropriate.
- Our review of all 28 Department users with access privileges to FRVIS program source code, parameters, Job Control Language (JCL), or data libraries as of June 14, 2017, disclosed inappropriate access privileges. Specifically, we found that:
  - 17 users were Department employees who had access to FRVIS program source code, parameters, and data libraries that was inappropriate for the users' job duties. In response to our inquiry, Department management stated that the access privileges would be removed for all 17 Department employees.
  - The access privileges for 2 former Department employees remained active for 55 and 745 days, respectively, after the employees separated from Department employment. In response to our inquiry, Department management stated that the access privileges for the 2 former Department employees would be removed.

The existence of inappropriate and unnecessary access privileges to FRVIS; the FRVIS database; database developer roles; or program source code, parameters, or data libraries increases the risk of unauthorized modification, loss, or disclosure of FRVIS data and related IT resources. Similar findings were noted in prior audits of the Department, most recently in our report No. 2014-183.

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.

Finding 2: Retention of Access Control Records

The 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 access control records related to the deactivation of employee access privileges from the FRVIS database.

The adequate retention of relevant access control records would promote management's assurance that the Department would have sufficient documentation to assist in future investigations of security incidents related to the FRVIS database, should they occur. A similar finding was noted in our report No. 2014-183.

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*.

Finding 3: Continuity of Operations

AST rules[4] require each agency to establish a procedure that ensures the agency's response and recovery plans are regularly tested and to ensure that security policies, processes, and procedures are maintained and used to manage the protection of information systems and assets. Also, the Division of Information Systems Administration's *Continuity of Operations Plan* (*COOP*) specifies testing and auditing requirements that include:

- Quarterly testing of the *COOP* to ensure the ability to perform mission-essential functions from alternate relocation points.
- Quarterly testing of interoperable communications from alternate work sites to ensure connectivity with databases, systems, hardware, and software.
- Conducting a formal audit of the *COOP* at least once a year.

Our audit procedures disclosed, however, that the Division of Information Systems Administration's Director, Bureau Chiefs, and Section and Office Supervisors had not conducted quarterly testing or an annual audit.

Appropriate and timely testing and audits of the *COOP* would increase management's assurance that critical Department operations would be timely and orderly resumed in the event of a disaster or other interruption of service.

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.

Finding 4: 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 procedures disclosed that certain security controls related to user authentication and logging and monitoring for FRVIS 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 FRVIS data and related IT resources. However, we have notified appropriate Department management of the specific

[4] AST Rule 74-2.003(5)(j), Florida Administrative Code.

issues. Similar issues were also communicated to Department management in connection with prior audits of the Department, most recently in our report No. 2014-183.

Without appropriate security controls related to user authentication and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of FRVIS data and IT resources may be compromised.

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.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report No. 2014-183.

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 January 2017 through April 2017 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 FRVIS during the period July 2016 through April 2017 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input and output; selected application-level general controls over logical access, change management, and contingency planning related to FRVIS; and applicable audit findings disclosed in audit report No. 2014-183. 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 our report No. 2014-083.
- 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 FRVIS-related documentation to obtain an understanding of:
  - The purpose and goals of FRVIS with respect to financial, operations, and compliance requirements.
  - The data and business process flows for FRVIS, including key sources of data input and key types of application data output related to FRVIS.
  - The Department's response to database outages that occurred during the audit period.
  - The FRVIS computing platform including applicable hardware, operating system, database management system, and security software related to the application and database.
- Evaluated FRVIS business process application controls related to input. Specifically, we:
  - Evaluated the Department's Division of Motorist Services' procedure documentation and the related quality assurance process and inquired of Department management to determine whether a procedure was in place for the processing and scanning of FRVIS supporting documents received from tax collector and tag agent offices.
  - Observed on March 2, 2017, at the Neil Kirkman Building, the processing and scanning of FRVIS supporting documents received from tax collector and tag agent offices.
  - Inspected two monthly missing image reports dated April 19, 2016, and one re-run monthly missing image report dated November 3, 2016; related correspondence dated December 7, 10, and 15, 2016, between the Division of Motorist Services and the tax collector and tag agent offices; and FRVIS *Title History Inquiry* screens on March 6, 2017, to determine

whether controls were in place for locating missing supporting documents received from tax collector and tag agent offices and whether the missing supporting documents were timely located.

- Evaluated FRVIS business process application controls related to output. Specifically, we:
  - Evaluated Department procedures and processes for vetting requesting parties and inquired of Department management to determine whether the requesting parties met the allowable reasons to access the information under the Federal Driver Protection Privacy Act (DPPA).
  - Inspected the *Memorandum of Understanding for Driver's License and Motor Vehicle Record Data Exchange* and related attachments for 25 requesting parties to determine whether controls were in place to ensure that the requesting parties met the conditions and limitations for the release of DPPA data.
- Evaluated Department change management procedures and other related documentation (i.e., *CM04 Change Management Policy V04, Change Management Procedure Workflows, Change Management in Service Manager User Guide, Division of Information Systems Administrative Information Systems Development Methodology, and How to use version control with Uniface*) and made inquiries to determine whether controls were in place to ensure that application changes were authorized and appropriate, and unauthorized changes were detected and promptly reported.
- Evaluated application contingency planning controls. Specifically, we:
  - Evaluated the Division of Information Systems Administration *Continuity of Operations Plan* (*COOP*) and the Department's *Disaster Recovery Plan* to determine whether controls had been established to ensure the execution of the Division's mission-essential functions in the event of an emergency or disaster.
  - Inspected the *COOP* and the *Disaster Recovery* Plan regarding required testing, as well as the *Immediate Response Information System Reports* screen for alerts and a Disaster Recovery Replication Testing e-mail dated October 18, 2016, and determined whether the Department conducted testing and auditing procedures required by *COOP*.
  - Inspected change management logs for October 2016 through February 2017, an enterprise system outage report for January 29, 2016, through February 16, 2017, and system availability reports for August 2016 through December 2016 to determine whether controls were in place to help prevent unexpected interruptions and identify recurring patterns or trends for FRVIS and evaluated the Department's response to database outages that occurred during the audit period.
  - Inspected the unsigned *Service-Level Agreement between the Department of Highway Safety and Motor Vehicles and the State of Florida Agency for State Technology*, inspected correspondence between Department staff and AST staff regarding the execution of the service-level agreement, and made inquiries with Department management to determine whether the agreement complied with Section 282.201(2)(d), Florida Statutes.
- Evaluated application access controls. Specifically, we:
  - Evaluated Division of Motorist Services *Procedure RS-64 & TL-57* and inspected documentation of the December 2016 periodic review of FRVIS-related user access privileges to determine whether adequate procedures were in place for the periodic review of FRVIS-related user access privileges.
  - Inspected various Department documents (i.e., FRVIS System Access and Roles – Annual Audit form letter; Alachua – FRVIS System Access Audit 2016 email dated December 1, 2016, with response dated December 2, 2016; List of FRVIS user roles; FRVIS Roles and Definitions for Tax Collectors; Tax Collector – FRVIS Access Authorization Request) and inquired of

Department management to determine whether FRVIS access privileges were periodically reviewed to help ensure the continued appropriateness of the access privileges granted.

  - Evaluated the appropriateness of the access privileges for 28 Department users with access privileges to FRVIS program source code, parameters, JCL, and data libraries as of June 14, 2017.
  - Evaluated the appropriateness of the access privileges for 9 active user IDs selected from the 41 active user IDs with the ability to directly update the FRVIS Oracle production database as of February 17, 2017.
  - Evaluated the appropriateness of the access privileges for 60 of the 5,287 active users with FRVIS access privileges as of April 11, 2017.
  - Evaluated the appropriateness of the access privileges for 75 active user IDs with a developer role that, as of February 17, 2017, granted update object access privileges to the FRVIS database tables.
  - Inquired of Department management and evaluated Department procedures and documentation for the retention of access control records to determine whether FRVIS-related records were retained, in accordance with the *General Records Schedule GS1-SL for State and Local Government Agencies*, for one anniversary year after being superseded or after the employee separated from Department employment to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
- Evaluated authentication controls for FRVIS and related IT resources.
- Evaluated the effectiveness of logging and monitoring controls related to FRVIS IT resources.
- 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

MANAGEMENT'S RESPONSE

Terry L. Rhodes
Executive Director

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

A SAFER
FLORIDA
HIGHWAY SAFETY AND MOTOR VEHICLES

October 5, 2017

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

Dear Ms. Norman:

Thank you for the opportunity to respond to the preliminary and tentative findings and recommendations from your audit of the Department of Highway Safety and Motor Vehicles Florida Real Time Vehicle Information System. 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,

Terry L. Rhodes
Executive Director

TLR/jl

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

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.

Agency 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.

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

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.

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.

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

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.