STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-089
January 2017

# DEPARTMENT OF FINANCIAL SERVICES

## Florida Accounting Information Resource Subsystem (FLAIR)


Sherrill F. Norman, CPA
Auditor General

## Chief Financial Officer

Pursuant to Article IV, Sections 4(c) and 5(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Jeff Atwater served as Chief Financial Officer during the period of our audit.

The team leaders were Andrew Denny, CISA, and Clark Evans, CPA, and the audit was supervised by Brenda Shiner, 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:

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 FINANCIAL SERVICES

## Florida Accounting Information Resource Subsystem (FLAIR)

## SUMMARY

This operational audit of the Department of Financial Services (Department) focused on evaluating selected information technology (IT) controls relevant to financial reporting and applicable to the Florida Accounting Information Resource Subsystem (FLAIR), and included a follow-up on the findings included in our report No. 2016-032, and Finding 6 in our report No. 2016-069. Our audit disclosed the following:

**Finding 1:** The access privileges for some FLAIR and network users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for assigned job duties.

**Finding 2:** The Department's procedures and processes for conducting periodic reviews of user access privileges need improvement to ensure access privileges assigned to users remain appropriate.

**Finding 3:** Certain security controls related to physical security, user authentication, and configuration management need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

## BACKGROUND

The Florida Accounting Information Resource Subsystem (FLAIR) is the State of Florida's accounting system. State law[1] establishes FLAIR as a subsystem of the Florida Financial Management Information System and the Department of Financial Services (Department) as the functional owner of FLAIR. The functions of FLAIR, as provided in State law,[2] include accounting and reporting so as to provide timely data for producing financial statements for the State in accordance with generally accepted accounting principles and for auditing and settling claims against the State.

FLAIR and the Department play a major role in ensuring that State financial transactions are accurately and timely recorded and that the State's Comprehensive Annual Financial Report (CAFR) is presented in accordance with appropriate standards, statutes, rules, and regulations.

FLAIR is composed of four components:

- The Departmental Accounting Component (DAC) maintains State agency accounting records and provides accounting details for general ledger transactions, account receivables, accounts payables, grants, projects, and assets. DAC provides State agency management with a budgetary check mechanism. The Statewide Financial Statements (SWFS) Subsystem of DAC is used to assist and support the Department's Division of Accounting and Auditing in the preparation of the State's CAFR. State agencies are the primary users of DAC.
- The Central Accounting Component (CAC) maintains a separate accounting system used by the Department on the cash basis for the control of the budget by line item of the General

[1] Sections 215.93(1)(b) and 215.94(2), Florida Statutes.

[2] Section 215.94(2), Florida Statutes.

Appropriations Act. CAC maintains the State of Florida's cash, budget, audit, tax reporting and payments. The Division of Accounting and Auditing is the primary user of CAC.

- The Payroll Component processes the State's payroll. The Division of Accounting and Auditing is the primary user of the Payroll Component. The Bureau of State Payrolls (BOSP) within the Division of Accounting and Auditing administers payroll processing.
- The Information Warehouse is a data storage and reporting system that allows users to access information extracted from DAC, CAC, the Payroll Component, and certain systems external to FLAIR. State agencies are the primary users of the Information Warehouse.

The Department is responsible for the operation and maintenance of FLAIR. Within the Department, the Division of Information Systems (DIS) operates the Chief Financial Officer's Data Center that maintains FLAIR.

In 2014, the Department, as the functional owner of FLAIR, created a multi-year project to replace FLAIR and the Department's Cash Management System (CMS) with a commercial off-the-shelf Enterprise Resource Planning (ERP) solution. The multi-year project is referred to as the Florida Planning, Accounting, and Ledger Management (Florida PALM) project. An Executive Steering Committee (ESC), together with the State CFO's Project Director, are responsible for Florida PALM project governance. The ESC consists of 15 members and includes representatives from multiple State Agencies.

The Florida PALM project is currently organized in three phases. As of May 2016, the Pre-Design, Development, Implementation (Pre-DDI) phase was in progress and expected to be completed in February 2018.

- Pre-DDI – This initial phase includes planning for DDI readiness, business process standardization, and procurement of the financial management software solution.
- DDI Phase 1 – The phase will implement the financial management software solution focusing on core functionality (at a minimum, functionality currently performed by the CAC, DAC, Payroll Component, Information Warehouse, and selected CMS functions).
- Future DDI Phases – Subsequent phases beyond what is defined for DDI Phase 1 (e.g., transition from Grant Accounting to full Grant Management functionality) will include the implementation of the remaining functionality necessary to meet the solution goals.

Pursuant to the 2016 General Appropriations Act,[3] the Department contracted with Computer Aid, Inc., to complete a business case for maintaining any of the agency business systems identified in the March 31, 2014, FLAIR study. The Department submitted the business case to the Executive Office of the Governor, President of the Senate, and Speaker of the House of Representatives on November 1, 2016. An initial draft Invitation to Negotiate for Software and Systems Integrator procurement was created and approved by the ESC on October 26, 2016. Subsequent to approval, the procurement process within the Pre-DDI phase will begin.

[3] Chapter 2016-066, Laws of Florida, Section 6, Specific Appropriation 2317A.

# FINDINGS AND RECOMMENDATIONS

## Finding 1: Appropriateness of Access Privileges

Effective access controls include measures that restrict access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Additionally, Department policy[4] requires that accounts with administrative rights be created, maintained, monitored, and removed in a manner that protects IT resources, and that administrative account activities be traceable to an individual. Furthermore, Department policy[5] requires access control administrators (ACA) to deactivate, by the close of business on the separation date, access assigned to employees voluntarily separating from Department employment. For involuntary separations, Department policy requires the Information Security Manager to ensure access to the Department's network is deactivated at the time of separation. Additionally, the ACAs are required to deactivate additional access privileges at the time of separation or as soon as possible upon receipt of the separation notification.

Our audit procedures disclosed some inappropriate and unnecessary access privileges for network administrative user accounts, a Payroll Component user account, and the Payroll Component program change management process. Specifically:

- **Network Administrative Account**. As of July 5, 2016, 1 of the 17 active administrative user accounts in the desktop administrative support group was shared by multiple individuals. This account was used for testing a specific application and had access privileges that allowed the joining of computers to a domain.[6] In response to our audit inquiry, Department management stated that as of August 8, 2016, the account was no longer being used and would be deactivated.
- **Payroll Component Function**. We evaluated the appropriateness of access for all 10 Statewide user accounts granted update access privileges during the period July 1, 2015, through May 31, 2016, to the tax reporting function within the Payroll Component of FLAIR. For 3 of the 10 user accounts evaluated, the assigned user terminated employment with the Department during the period July 1, 2015, through May 31, 2016. For 1 of the 3 user accounts assigned to a former employee, we determined that the update access privileges to the tax reporting function were not timely deactivated and remained active for 4 days after the employee's separation date. In response to audit inquiry, Department staff stated that the former employee's access was not used after the employee's separation date. A similar issue was noted in our report No. 2016-032.
- **Payroll Component Program Change Management**. Our audit procedures disclosed that, as of June 17, 2016, all seven employees in the Division of Information Systems (DIS) with the ability to implement program files into the Payroll Component production environment also had the ability to make program changes within the development environment, contrary to an appropriate separation of duties. In response to our audit inquiry, Department management stated that a daily report was generated listing programs implemented into production for the prior day and reviewed by Department management to ensure that only approved programs were implemented into production. However, our review of the report as of June 20, 2016, disclosed that the report provided only the name of the program file that changed and did not contain the specific code

[4]Administrative Policies and Procedures, Information Technology Security Policy 4-03.

[5]Administrative Policies and Procedures, Application Access Control Policy 4-05.

[6]A domain is a form of a computer network in which all user accounts, computers, printers and other security principles, are registered with a central database located on one or more clusters of central computers known as domain controllers.

changes for review. Department management further stated an additional review process that included a detailed review of the changed source code by another programmer not associated with the change may be performed before implementation into the production environment but that no written policies and procedures requiring source code review existed. A similar issue was noted in our report No. 2016-032.

Inappropriate or unnecessary access privileges increase the risk of unauthorized modification, loss, or disclosure of data and IT resources. Additionally, shared accounts limit management's ability to trace activities to a specific individual.

**Recommendation: We recommend that Department management improve controls to ensure that user accounts are uniquely assigned, timely deactivated when no longer needed or an employee terminates or transfers, and promote an appropriate separation of duties.**

## Finding 2: Periodic Review of User Access Privileges

Effective access controls include procedures for the periodic reviews of user access privileges based on risk, access account change activity, and error rate. Periodically conducting reviews of user access privileges helps ensure that only authorized users have access and that the access provided to each user remains appropriate.

Our audit disclosed that Department procedures and processes for the periodic review of user access privileges for specific users need improvement. Specifically, we noted that:

- The *Access Control Business Process Procedure* (*Procedure*) used for authorizing and reviewing DAC user access privileges for operating level organization (OLO) 4390 was last updated in June 2013. As of July 20, 2016, one position number in the *Procedure* was listed as the designated Access Control Custodian for OLO 4390 and authorized for the corresponding user access privileges. However, this position had been moved to a different area within the Department and no longer required access as an Access Control Custodian. Additionally, we determined that one of the current positions authorized as the Access Control Custodian was not documented in the *Procedure*.
- As of August 3, 2016, periodic reviews of privileged administrator account access privileges in the network environment, including domain administrator accounts, had not been performed.
- Although Department procedures required periodic reviews of COmmon Business-Oriented Language (COBOL) user access privileges by the users' supervisors, Department records as of June 22, 2016, did not evidence that periodic reviews had been conducted by the users' supervisors. A similar issue was noted in our report No. 2016-032.
- As of August 31, 2016, the Department's procedures for periodic review of user access privileges did not include the Statewide user access privileges defined for the DAC State Chief Financial Officer Files (SC) function and the related DAC SC Electronic Funds Transfer (EFT) Authorization Inquiry Request (ET) mini-menu function. A similar issue was noted in our report No. 2016-032.

Up-to-date access review procedures facilitate effective review of user access privileges. Additionally, periodic reviews of user access privileges reduce the risk that inappropriate access to programs and data may exist that could result in comprised data integrity.

**Recommendation: We recommend that Department management ensure that access control procedures are up to date, all periodic reviews are performed as required and include all assigned user access privileges, and documentation of completed reviews is maintained.**

### Finding 3: Security Controls – Physical Security, User Authentication, and Configuration Management

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 physical security, user authentication, and configuration management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of Department data and IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to physical security, user authentication, and firewall configuration management, the risk is increased that the confidentiality, integrity and availability of Department data and IT resources may be compromised. A similar finding related to network authentication was communicated to Department management with our report No. 2016-069.

**Recommendation: We recommend that Department management improve certain security controls related to physical security, user authentication, and configuration management to ensure the confidentiality, integrity, and availability of Department data and 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 Nos. 2016-032 and 2016-069.

## 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 June 2016 through September 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 FLAIR and relevant to financial reporting during the period July 2015 through June 2016 and selected actions subsequent thereto. The audit included selected business process application controls related to voucher processing interface files, manual transactions, and selected payroll transaction data input, processing, and output applicable to financial reporting. The audit also included selected application-level and other general IT controls over logical and physical access, firewall, and configuration management.

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. 2016-032 and Finding 6 in audit report No. 2016-069.
- 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 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 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 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 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 to obtain an understanding of the data flow of FLAIR including Central, Departmental and Payroll component processing, FLAIR and network device change control processes, logical access and user authentication controls for FLAIR and the Department's interconnected network.
- Interviewed Department personnel and reviewed relevant documentation to obtain an understanding of the Department's strategic IT planning process and to determine the status of the Florida PALM project.
- Interviewed personnel and reviewed applicable documentation related to 2 of the 11 planned FLAIR major enhancements and 1 of 13 implemented enhancements identified on the Department's response to the Auditor General's information technology entity survey dated

March 7, 2016, to determine whether there would be a potential impact on financial reporting from a Statewide financial statement perspective.

- Interviewed personnel and reviewed applicable documentation as of November 9, 2016, to determine the implementation status and the impact to FLAIR of the Department's initiative to change the vendor for the Cash Management System Concentration Account, which is a centralized financial institution account for State deposits.
- Obtained an understanding of the DAC voucher processing flow in FLAIR to determine the types of transactions input through interface files and the controls established to ensure the interface file transactions are valid.
- Evaluated user authentication controls related to the Department's network as of June 14, 2016.
- Observed on July 29, 2016, the online input control for 1 of the 8 disbursement transaction types that ensures the offsetting entry in FLAIR is system-generated and cannot be overridden by the user.
- Evaluated the effectiveness of firewall change controls related to system logging and documentation of changes. Additionally, we evaluated the effectiveness of firewall firmware patch management controls for 4 of the 15 physical firewall devices as of August 12, 2016.
- Evaluated the effectiveness of the Department's criminal background screening process for all 7 BOSP employees who were assigned global user access privileges to the Report Distribution System (RDS) reports as of June 15, 2016.
- Evaluated the effectiveness of the beginning pay date input control for the On-Demand Payroll Component as of September 29, 2016.
- Evaluated procedures for ensuring the completeness, accuracy, and availability of payroll adjustments for refunds and recoupments processed through variance invoices, as well as the updating of employee records related to variance invoices in the Payroll Component of FLAIR. Specifically, we:
    - Evaluated the timeliness of processing employee refund adjustments listed on variance invoices for all 598 adjustments received during the period July 1, 2015, through June 30, 2016.
    - Evaluated the timeliness of follow-up for 5 of the 43 incomplete employee refund adjustments listed on variance invoices received during the period July 1, 2015, through June 30, 2016.
- Evaluated the access privileges granted to all 7 DIS Payroll component programmers as of June 17, 2016, to determine whether the access privileges granted promoted an appropriate separation of duties between the development of Payroll component changes and the implementation of Payroll component changes into the production environment.
- Interviewed Department staff and inspected the 2016 Department Disaster Recovery Plan (DR Plan) to gain an understanding of the Department's disaster recovery procedures and evaluated the effectiveness of the DR Plan to ensure it included required components such as identifying critical systems, continuity of operations plans for the resumption of critical operations in the event of a disaster or interruption in service, off-site processing facility, and annual testing of the DR Plan.
- Evaluated the appropriateness of physical access controls implemented at the Department's Data Center to protect its IT resources and data, including the appropriateness of access and the periodic review of physical access to the Data Center and DIS secured areas.
- Evaluated the appropriateness of physical access privileges to the Data Center and DIS secured areas for all 65 active key cards as of June 16, 2016.

- Evaluated the effectiveness of selected logical access controls for FLAIR and underlying infrastructure. Specifically, we evaluated the:
  - The appropriateness of access privileges for all 3 BOSP users with access privileges to the DAC cash receipts (CR) and cash disbursements (DB) functions as of May 31, 2016.
  - The appropriateness of Statewide access privileges for the DAC SC function for all 10 users assigned access privileges as of May 31, 2016.
  - The appropriateness of Statewide access privileges to the DAC SC ET mini-menu function for all 6 users assigned access privileges as of May 31, 2016.
  - The appropriateness of access privileges for all 43 network user accounts with administrative access privileges, including domain administrator accounts, help desk accounts, and desktop support accounts as of July 5, 2016.
  - The appropriateness of access privileges for all 14 Resource Access Control Facility (RACF) accounts with membership in the RACF group with the ability to grant and modify access to Adabas as of June 22, 2016.
  - The appropriateness of access privileges for all 19 user accounts defined as system administrators in the DB2 database as of August 9, 2016, to determine whether access to grant and modify functions was appropriate.
  - The appropriateness of high-risk administrative access privileges (SPECIAL privilege) for 21 of 33 RACF user groups as of June 15, 2016.
  - The appropriateness of access privileges for all 3 user accounts with Natural Security administrative privileges to 5 of 10 FLAIR DAC and CAC production databases as of June 30, 2016.
  - The appropriateness of access privileges for all 12 Natural Security administrator accounts within the DAC development environment and all 6 Natural Security administrator accounts within the CAC development environment as of June 30, 2016.
  - The appropriateness of access privileges for all 10 user accounts with Statewide update privileges to tax reporting function in FLAIR between July 1, 2015, and May 31, 2016.
- Evaluated the effectiveness of periodic access review processes for FLAIR and the underlying infrastructure. Specifically we evaluated:
  - The periodic reviews of user access privileges for the COBOL, RACF, Natural Security, UNIX, Adabas, and DB2, and network environments.
  - BOSP periodic reviews of user access privileges for the CR and DB functions within DAC.
  - BOSP periodic reviews of user access privileges to the tax reporting function in the Payroll Component.
  - The periodic reviews of user access privileges to the RDS.
  - The periodic reviews of user access privileges to DAC State CFO Files (SC) function and related SC ET Mini-Menu function.
- 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

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

January 4, 2017

Sherrill F. Norman
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's information technology operational audit of the *Department of Financial Services, Florida Accounting Information Resource Subsystem (FLAIR).*

If you have any questions concerning this response, please contact Teresa Michael, Inspector General, at (850) 413-3112.

Sincerely,

Jeff Atwater

JA:rlg

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 FAX (850) 413-2950

**DEPARTMENT OF FINANCIAL SERVICES**
**FLORIDA ACCOUNTING INFORMATION RESOURCE SUBSYSTEM (FLAIR)**
**Information Technology Operational Audit**

## RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

### Finding No. 1: Appropriateness of Access Privileges

The access privileges for some FLAIR and network users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for assigned job duties.

**Recommendation:** Department management should improve controls to ensure that user accounts are uniquely assigned, timely deactivated when no longer needed or an employee terminates or transfers, and promote an appropriate separation of duties.

**Response:** We concur. The Division of Accounting and Auditing will improve controls to ensure that user accounts are uniquely assigned and timely deactivated. The Office of Information Technology (OIT) terminated the shared desktop administrative account on September 26, 2016. Additionally, OIT implemented documented procedures for the payroll component program change management review process on December 1, 2016.

**Expected Completion Date for Corrective Action:** Accounting and Auditing - July 1, 2017; OIT - corrective action was completed as of December 1, 2016.

## Finding No. 2: Periodic Review of User Access Privileges

The Department's procedures and processes for conducting periodic reviews of user access privileges need improvement to ensure access privileges assigned to users remain appropriate.

**Recommendation**: Department management should ensure that access control procedures are up to date, all periodic reviews are performed as required and include all assigned user access privileges, and documentation of completed reviews is maintained.

**Response:** We concur. The Division of Accounting and Auditing will update DACA for OLO 4390 Access Control Business Process Procedure used for authorizing and reviewing DAC user access privileges. On October 6, 2016, OIT implemented a process for quarterly reviews of privileged administrator accounts and the first quarterly review was completed on October 28, 2016. Additionally, on October 11, 2016, OIT modified the COBOL access review process to include tracking of review responses. The OIT also submitted a change request on November 29, 2016, to incorporate an additional report into the DAC access review process which includes the additional access levels.

**Expected Completion Date for Corrective Action:** Accounting and Auditing - July 1, 2017; OIT - pending OIT corrective action anticipated to be completed by February 28, 2017.

**Finding No. 3: Security Controls – Physical Security, User Authentication, and Configuration Management**

Certain security controls related to physical security, user authentication, and configuration management need improvement to ensure the confidentiality, integrity, and availability of Department data and IT resources.

**Recommendation:** Department management should improve certain security controls related to physical security, user authentication, and configuration management to ensure the confidentiality, integrity, and availability of Department data and IT resources.

**Response:** As of October 19, 2016, OIT concluded implementation of corrective action to address physical security related concerns. The OIT will evaluate the additional security concerns and, where appropriate, implement additional controls.

**Expected Completion Date for Corrective Action:** OIT corrective action evaluation anticipated to be completed by March 30, 2017.