STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-068
December 2018

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 Jimmy Patronis served as Chief Financial Officer during the period of our audit.

The team leader was Clark Evans, CPA, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

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 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 applicable to financial reporting and applicable to the Florida Accounting Information Resource Subsystem (FLAIR). Our audit included a follow-up on the findings included in our report No. 2018-025. Our audit disclosed the following:

Finding 1: The Department did not timely deactivate the FLAIR user accounts with access privileges to the Central Accounting Component and Payroll Component for some former or suspended employees. A similar finding was noted in our report No. 2018-025.

Finding 2: Change management controls related to hardware and systems software changes for high-risk network devices related to FLAIR need improvement to ensure that only approved hardware and systems software changes are implemented into the production environment. A similar finding was noted in our report No. 2018-025.

Finding 3: As similarly noted in our report No. 2018-025, the Department had not established a comprehensive policy for the performance of background screenings of employees and contracted consultants in positions of special trust. Additionally, background screening processes for contracted consultants need improvement to ensure all consultants are screened prior to the start of the contract and that evidence of the background screenings is maintained.

Finding 4: Certain security controls related to physical security, logical access, user authentication, logging and monitoring, and configuration management continue to need improvement to ensure the confidentiality, integrity, and availability of FLAIR data and other Department 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 stated 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 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.

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

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

FLAIR is composed of four components:

- The Departmental Accounting Component (DAC) maintains State agency accounting records and provides accounting details for general ledger transactions, accounts receivable, accounts payable, 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 the State of Florida's checkbook used by the Department to process payments for the State. CAC is a cash-basis system for the control of budget by line item of the General Appropriations Act. The primary user of CAC is the Division of Accounting and Auditing.
- 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 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 Office of Information Technology (OIT), 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 Subsystem (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 Florida PALM 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 into three phases:

- Pre-Design, Development, Implementation (Pre-DDI) phase – This initial phase included planning for DDI readiness, business process standardization, and procurement of the financial management software solution. This phase of the Florida PALM project was completed in June 2018.
- DDI Phase 1 – This phase will implement the financial management software solution focusing on core functionality (at a minimum, functionality currently performed by the FLAIR CAC, DAC, Payroll Component, Information Warehouse, and selected CMS functions).
- DDI Phase 2 – This phase will implement expanded functionality beyond what is defined for DDI Phase 1 (e.g., transition from Grant Accounting to full Grant Management functionality) to meet the solution goals.

Pursuant to the 2016 General Appropriations Act,[3] the Department contracted with Computer Aid, Inc. (CAI), 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 CAI *Business Case for Maintaining Agency*

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

Business Systems to the Executive Office of the Governor, President of the Senate, and Speaker of the House of Representatives on November 1, 2016.

The Department issued an Invitation to Negotiate (ITN) for Software and System Integrator Services for the Florida PALM project on November 1, 2016. In October 2017, all three respondents within the competitive range were invited to negotiate with the Department. On June 15, 2018, the negotiation team recommended awarding the contract for Software and System Integrator Services to Accenture, LLP. On June 19, 2018, the Chief Financial Officer signed a memorandum recommending the award and an Intent to Award was issued.

A Pre-DDI Closeout Report was issued on June 29, 2018, which concluded the Pre-DDI phase. After the Intent to Award was issued, two notices of intent to protest the award were filed resulting in one formal protest on July 2, 2018, and the Florida PALM project initiated an interim schedule. Subsequently, the protest was officially withdrawn, and the Florida PALM project entered DDI Phase 1 by executing a contract with Accenture, LLP on July 20, 2018, for Software and System Integrator Services.

FINDINGS AND RECOMMENDATIONS

Finding 1: Timely Deactivation of Access Privileges

Effective management of IT access privileges includes the timely deactivation of employee IT access privileges when an employee separates or is suspended from employment. Prompt action is necessary to ensure that the access privileges are not misused by former employees or others to compromise data or IT resources. Department policy[4] requires that accounts with administrative rights be created, maintained, monitored, and removed in a manner that protects IT resources. Department policy[5] also states that access shall be granted on the principles of least privilege and a need-to-know basis and requires access control administrators 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 designated time of the involuntary separation.

Our audit procedures disclosed that the FLAIR user accounts for some former or suspended employees were not timely deactivated upon an employee's separation or suspension from Department employment. Specifically:

- We evaluated whether the FLAIR user accounts were timely deactivated for the 12 former employees with CAC access privileges who separated from Department employment during the period July 1, 2017, through April 30, 2018. We determined that the user accounts for 3 of the 12 former employees with CAC access privileges were not timely deactivated and remained active from 1 to 6 days after the employees separated from Department employment. In response to our audit inquiry, Department management stated that the access privileges were not timely deactivated for 2 of the user accounts because the Access Control Custodian had been out of the office and the backup custodian failed to complete the deactivation. A similar finding was noted in our report No. 2018-025.

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

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

- We evaluated the 162 active FLAIR user accounts with CAC access privileges as of April 30, 2018, to determine whether any active user accounts were assigned to vacant positions. We determined that 1 active user account with CAC access privileges was assigned to a vacant position and was not traceable to an individual with a valid business purpose. This user account had not been removed, disabled, or otherwise secured, and also possessed update access to the Journal Transfer Audit Detail, Voucher Audit Detail, and Special Flag Override functions. In response to our audit inquiry, Department management indicated they had followed the access control process in place at the time the position was vacated and that the user account would not be accessible without contacting the Access Control Custodian. Notwithstanding this response, the active FLAIR user account could be accessed by a Department network user in the event the account credentials were compromised.
- We evaluated whether FLAIR user accounts were timely deactivated for the seven employees with Statewide access privileges to the Payroll Component who separated from Department employment or were placed on suspension during the period July 1, 2017, through April 30, 2018. We found that the user accounts for 2 of the 6 former employees with Statewide access privileges to the Payroll Component were not timely deactivated and remained active for 7 and 104 days after the employees separated from Department employment. Additionally, for the employee who was placed on suspension, the access privileges remained active during the suspension period. In response to our audit inquiry, Department management indicated that the access privileges were not timely deactivated for 2 of the user accounts because the Access Control Custodian was not timely notified by the supervisors and the other user account was not timely deactivated because the Access Control Custodian was on leave at the time of notification. A similar finding was noted in our report No. 2018-025.

Timely deactivation of FLAIR user accounts upon an employee's separation or suspension from Department employment reduces the risk that CAC and Payroll Component access privileges may be misused by the former or suspended employee or others.

Recommendation: We recommend that Department management ensure that the FLAIR user accounts with CAC and Payroll Component access privileges for former or suspended employees are timely deactivated upon the employee's separation or suspension from Department employment.

Finding 2: Change Management Controls

Effective change management controls over modifications to hardware and systems software ensure that only approved changes are implemented into the production environment. Department procedures[6] require all inbound and outbound traffic change requests for high-risk network devices to be evaluated by both the Network Services team and the Information Security Office (ISO) to ensure the changes conform to current security best practices and OIT security policies. Additionally, Department procedures[7] require standard changes that are relatively common and follow a procedure or work instruction be preapproved.

As part of our audit, we evaluated 22 of the 208 change requests related to high-risk network devices that were implemented into the production environment during the period July 1, 2017, through May 31, 2018, to determine whether high-risk network device change requests were appropriately approved at all required levels prior to being implemented into the production environment. We noted

[6] Office of Information Technology – OIT Operating Procedures, OIT-028.

[7] Office of Information Technology – OIT Operating Procedures, OIT-015.

that, for 5 of the 22 high-risk network device change requests evaluated, approval did not occur at all required levels. Specifically, for the 2 change requests that related to inbound and outbound traffic, 1 lacked the required ISO approval and the other lacked any approvals. For the remaining 3 change requests, while ISO approval was not necessary, the Department lacked documentation of any approvals for the changes. A similar finding was noted in our report No. 2018-025.

Effective change management controls ensure that all hardware and systems software changes are appropriately documented to evidence that changes are approved. Without proper controls including approval, the risk is increased that erroneous or unauthorized changes may be implemented into the production environment.

Recommendation: We again recommend that Department management improve change management controls to ensure that approvals are appropriately documented for all high-risk network device changes prior to implementation into the production environment.

Finding 3: Background Screenings

Effective security controls include the performance of security background screenings upon hire and periodically thereafter for personnel in sensitive or special trust positions. Such positions typically include IT personnel with elevated access privileges or responsibilities for the custody of sensitive IT resources. Additionally, State law[8] requires each State agency to designate positions which, because of the special trust, responsibility, or sensitive location, require security investigations (i.e., background screenings). All persons and employees in such positions must undergo background screenings, including fingerprinting, as a condition of employment and continued employment.

In report No. 2018-025 (Finding 4), we noted that the Department had not established a comprehensive policy for background screenings that required the periodic performance of background screenings for personnel and contracted consultants in positions of special trust. In response to that Finding, Department management indicated that a Departmentwide background screening policy was being developed that included the requirement for periodic screenings and requirements for screening employees prior to hire and upon transfer. The draft policy also required contracted consultants to be screened prior to hire and every 2 years. As part of our follow-up audit procedures, we examined the Department's policies and procedures and noted that as of September 10, 2018, the Departmentwide background screening policy continued to be in development. While the Department only had a draft policy for background screenings, the Department had a process that required new employees and contractors hired into positions of special trust to be screened as a condition of employment and employees transferring to a position of special trust be screened if it had been more than 6 months since their last screening.

We evaluated background screening reports for 11 of the 41 OIT contracted consultants requiring background screening as a condition of providing services to the OIT as of June 27, 2018. Our audit procedures disclosed that documentation of the required background screenings for 7 of the 11 selected

[8] Section 110.1127(2)(a), Florida Statutes.

contracted consultants providing services to the OIT was not available or evidenced that the screenings were performed late. Specifically, we noted that, as of June 27, 2018:

- For 2 of the 7 contracted consultants, the required background screening had not been performed. The contracts for these consultants began on May 17, 2017, and July 1, 2017, respectively.
- For 3 of the 7 contracted consultants, while background screenings were performed in June 2014 for contracts that ended in 2016, a background screening had not been performed for the current contracts. The contracts for 2 of the consultants began on August 27, 2017, and the other consultant's contract began on September 1, 2017.
- Background screenings for the other 2 contracted consultants were performed; however, the screenings were performed 22 and 256 days, respectively, after the start of the contracts.

Without a comprehensive Departmentwide background screening policy and effective procedures, the risk is increased that people with inappropriate backgrounds may be employed in positions of special trust and may gain access to confidential or sensitive data and IT resources.

Recommendation: We again recommend that Department management continue efforts to establish a comprehensive Departmentwide background screening policy and related procedures and ensure the timely performance of background screenings of contracted consultants in positions of special trust.

Finding 4: Security Controls – Physical Security, Logical Access, User Authentication, Logging and Monitoring, 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, logical access, user authentication, logging and monitoring, and configuration management need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FLAIR data and other Department IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to physical security, logical access, user authentication, logging and monitoring, and configuration management, the risk is increased that the confidentiality, integrity, and availability of FLAIR data and other IT resources may be compromised. Similar findings were communicated to Department management in connection with our report No. 2018-025.

Recommendation: We again recommend that Department management improve certain security controls related to physical security, logical access, user authentication, logging and monitoring, and configuration management to ensure the confidentiality, integrity, and availability of FLAIR data and other Department 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. 2018-025.

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 May 2018 through August 2018 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 relevant to financial reporting and applicable to FLAIR during the period July 2017 through June 2018 and selected actions thereto.

The overall objectives of the audit were:

- To evaluate 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. 2018-025.
- 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 and reviewed related documentation to obtain an understanding of:
  - Logical access controls and the paths and methods for authenticating to FLAIR, and the Department's network and underlying infrastructure.
  - Configuration management processes for the Department's network and underlying infrastructure.
  - Physical access controls for the Department's Data Center and OIT-secured areas.
  - Background screening processes for Department employees and contracted consultants in positions of special trust.
  - Business processes for FLAIR, including daily operations and maintenance for the FLAIR DAC Purchasing Card Module.
  - The strategic IT planning process and status of the Florida PALM project.
- Examined and evaluated the procedures for processing the electronic data interface (EDI) upload to the DAC Purchasing Card Module to ensure the EDI files are reviewed timely and errors are identified and resolved to ensure the Module is available for Statewide users.
- Observed on June 14, 2018, the Department's physical security control processes implemented for OIT-secured areas to determine whether access to sensitive areas and IT resources was appropriately restricted.
- Evaluated user authentication controls related to FLAIR, and the Department's network and underlying infrastructure, and documentation of the risk acceptance related to user authentication controls for the Department's network.
- Evaluated the effectiveness of the Department's logging and monitoring controls related to FLAIR, and the Department's network and underlying infrastructure.
- Evaluated the logical design, appropriateness, and administration procedures for logical access privileges to FLAIR, FLAIR's underlying infrastructure, and the Department's network infrastructure. Specifically, we evaluated:
  - The appropriateness of access privileges for 10 of the 92 users with update access privileges to 1 or more of 16 key CAC FLAIR functions as of April 30, 2018.
  - Whether any of the 162 active CAC user accounts as of April 30, 2018, were assigned to a vacant position.
  - The appropriateness of access privileges for the 20 users with update or inquiry access privileges to three confidential CAC electronic funds transfer (EFT) functions, EFT Authorization File; EFT Payment Detail; and EFT Bank Title File, as of April 30, 2018.
  - The appropriateness of access privileges as of April 30, 2018, for the 31 users with update or override access privileges to 40 key Payroll Component functions and directory tables for the Statewide Payroll Component of FLAIR.

- The timely deactivation of CAC access privileges for the 12 former employees with CAC access who separated from the Department during the period July 1, 2017, through April 30, 2018.
- The timely deactivation of Payroll Component Statewide access privileges for the six former employees who separated from the Department, and one employee suspended from employment during the period July 1, 2017, through April 30, 2018.
- The appropriateness of access privileges for the 82 network user accounts as of May 21, 2018, with either network administrative access privileges, help desk support access privileges, desktop support access privileges, or network server administrative access privileges.
- The appropriateness of access privileges for the 41 network user accounts with global administrative privileges on Department workstations in two selected high-risk security groups in the Department's network domain as of July 17, 2018.
- The appropriateness of access privileges for the 26 administrative accounts among 13 selected high-risk network devices as of June 1, 2018, and June 27, 2018.
- Whether the access privileges granted as of June 28, 2018, promoted an appropriate separation of duties between the development of Payroll Component changes and the implementation of Payroll Component changes into the production environment.
- The logical access controls over the protection of the confidential data in the Payroll Component test environment used for program development and testing as of June 28, 2018.

- Evaluated the effectiveness of periodic access review processes for FLAIR, and the Department's network and underlying infrastructure. Specifically, we evaluated the adequacy of periodic reviews of user access privileges:
  - To the network and related environments.
  - Of CAC users and users with Statewide access to the Payroll Component of FLAIR.
  - To DAC State CFO Files (SC) function and the related DAC SC EFT Authorization Inquiry Request (ET) mini-menu function.
  - To DAC utilized by the Division of Accounting and Auditing (OLO 4390).
- Evaluated the appropriateness of physical access controls implemented at the Department's Data Center to protect its IT resources and data. Specifically, we evaluated:
  - The appropriateness of physical access privileges to the Data Center and OIT-secured areas for the 86 active key cards as of June 19, 2018.
  - The adequacy of the quarterly access reviews of physical access privileges to the Data Center and OIT-secured areas for July 2017 through April 2018.
- Evaluated the effectiveness of change controls for 22 of the 208 high-risk network device changes implemented into production during the period July 1, 2017, through May 31, 2018.
- Evaluated the effectiveness of patch management controls for the 13 high-risk network devices to evaluate whether, as of June 1, 2018, and July 30, 2018, the Department had timely installed vendor-supplied patches.
- Examined and evaluated the Departmentwide and OIT background screening policies and procedures providing for the performance of background screenings for employees and contracted consultants in positions of special trust.

- Evaluated the timeliness of background screenings for 18 of 138 OIT employees in positions of special trust as of June 30, 2018, and for 11 of the 41 contracted consultants providing services to the OIT as of June 27, 2018.
- 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
JIMMY PATRONIS
STATE OF FLORIDA

December 4, 2018

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 *Florida Accounting Information Resource Subsystem (FLAIR)*.

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

Sincerely,

Jimmy Patronis

JP/hm
Enclosure

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

Florida Accounting Information Resource Subsystem (FLAIR) Information Technology Operational Audit

DEPARTMENT OF FINANCIAL SERVICES' RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Timely Deactivation of Access Privileges

The Department did not timely deactivate the FLAIR user accounts with access privileges to the Central Accounting Component and Payroll Component for some former or suspended employees. A similar finding was noted in our report No. 2018-025.

Recommendation: We recommend that Department management ensure that the FLAIR user accounts with CAC and Payroll Component access privileges for former or suspended employees are timely deactivated upon the employee's separation or suspension from Department employment.

Response: We concur.

The Division of Accounting and Auditing (A&A) is working on updating procedures to ensure timely deactivation of access privileges. The Division is also coordinating efforts with the Division of Administration to suspend or terminate access control privileges when an employee is either suspended or terminated in an appropriate manner.

Expected Completion Date for Corrective Action: December 31, 2018

Florida Accounting Information Resource Subsystem (FLAIR) Information Technology Operational Audit

Finding No. 2: Change Management Controls

Change management controls related to hardware and systems software changes for high-risk network devices related to FLAIR need improvement to ensure that only approved hardware and systems software changes are implemented into the production environment. A similar finding was noted in our report No. 2018-025.

Recommendation: We again recommend that Department management improve change management controls to ensure that approvals are appropriately documented for all high-risk network device changes prior to implementation into the production environment.

Response: We concur.

The Office of Information Technology (OIT) polices will be revised to more granularly define the approval process. Specifically, OIT policy OIT-028 will be revised to reflect that only access control list (ACL) changes need to go through the change management process.

Expected Completion Date for Corrective Action: May 31, 2019

Finding No. 3: Background Screenings

As similarly noted in our report No. 2018-025, the Department had not established a comprehensive policy for the performance of background screenings of employees and contracted consultants in positions of special trust. Additionally, background screening processes for contracted consultants need improvement to ensure all consultants are screened prior to the start of the contract and that evidence of the background screenings is maintained.

Recommendation: We again recommend that Department management continue efforts to establish a comprehensive Departmentwide background screening policy and related procedures and ensure the timely performance of background screenings of contracted consultants in positions of special trust.

Response: We concur.

The Division of Administration will continue its efforts to establish a comprehensive Departmentwide background screening policy and related procedures, both of which will be designed to ensure the timely performance of background screenings of employees and contracted consultants, being designated into positions of special trust.

Expected Completion Date for Corrective Action: May 31, 2019

Finding No. 4: Security Controls – Physical Security, Logical Access, User Authentication, Logging and Monitoring, and Configuration Management

Certain security controls related to physical security, logical access, user authentication, logging and monitoring, and configuration management continue to need improvement to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

Recommendation: We again recommend that Department management improve certain security controls related to physical security, logical access, user authentication, logging and monitoring, and configuration management to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources.

Response: The OIT has performed some corrective action to address security controls. The OIG will continue to monitoring OIT's and A&A's efforts until documentation is provided that demonstrates security controls related to physical security, logical access, user authentication, logging and monitoring are improved.

Expected Completion Date for Corrective Action: May 31, 2019