STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2021-131
February 2021

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource Subsystem (FLAIR) and Selected Information Technology Controls



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, Jr., CPA, CISA, and the audit was supervised by Suzanne B. Varick, CPA.

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) and Selected Information Technology Controls

SUMMARY

This operational audit of the Department of Financial Services (Department) focused on the Florida Accounting Information Resource Subsystem (FLAIR) and selected information technology (IT) controls. The audit also included a follow-up on the findings included in our report No. 2020-095 and, as applicable to the scope of this audit, Finding 6 included in our report No. 2020-056. Our audit disclosed the following:

Finding 1: Department procedures for assigning Statewide access privileges to the FLAIR Payroll Component need improvement.

Finding 2: As similarly noted in prior audit reports, most recently in our report No. 2020-095, the Department had not established a comprehensive policy for the performance of background screenings of employees and contractors in positions of special trust. Additionally, background screening processes for contractors continue to need improvement to ensure that all contractors are screened prior to the start of contracted work.

Finding 3: The Department did not conduct periodic access reviews of the administrative accounts on the Department's network domain.

Finding 4: Certain Department security controls related to physical access, logical access, user authentication, and logging and monitoring 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. As provided in State law,[2] the functions of FLAIR include accounting and reporting 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, rules, regulations, and statutes.

FLAIR is composed of four components:

- The Departmental Accounting Component (DAC), which maintains State agency accounting records and provides accounting details for general ledger transactions, accounts receivable,

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

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

accounts payable, grants, projects, and assets. DAC provides State agency management with a budgetary check mechanism. The Statewide Financial Statements Subsystem of DAC and the Wdesk application are used to assist and support the Department, 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), which 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, which 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, which is a reporting system that allows users to access information extracted from DAC, CAC, the Payroll Component, and certain systems external to FLAIR. The primary users of the Information Warehouse are State agencies, the Division of Accounting and Auditing, and the Department's Office of Information Technology (OIT).

The Department is responsible for the design, implementation, and operation of FLAIR. Within the Department, the OIT operates the Chief Financial Officer's Data Center and maintains FLAIR.

In 2014, the Department, as the functional owner of FLAIR, created the Florida Planning, Accounting, and Ledger Management (Florida PALM) project to replace FLAIR and most of the applications within the Treasury Cash Management Subsystem (CMS)[3] with a cloud-based financial management solution to modernize the State's financial management processes and system. As shown in Table 1, beginning in 2021 and through 2026, this multi-year project is to transition FLAIR and CMS functions, as well as additional functionality, to the Florida PALM System, with production support commencing upon implementation of initial functionality.

Table 1
Florida PALM System Transition Timeline

Function	Description	Planned Transition Date
CMS	Cash management functions	July 2021
CAC	State budgeting functions	July 2022
Payroll	Payroll functions	January 2024
DAC	State agencies' accounting records and budget management functions	July 2024
Additional	Additional functionality for all agencies	2026

Source: Melissa Turner, Project Director, Florida PALM Project, as of November 24, 2020.

The Department will continue operating FLAIR and CMS until all agencies are fully transitioned to the Florida PALM System. An Executive Steering Committee, together with the Florida PALM Project

[3] The CMS includes the CMS application, Fund Accounting, Dis-Investments, Consolidated Revolving Account, Bank Accounts, Warrant Processing, Investment Accounting, State Accounts, Archive, Special Purpose Investment Account (SPIA), and Certificates of Deposits (CD). Florida PALM replaces eight of these applications, excluding Archive, SPIA, and CD.

Director, are responsible for Florida PALM project governance. The Executive Steering Committee consists of 15 members and includes representatives from multiple State agencies.

FINDINGS AND RECOMMENDATIONS

Finding 1: Access Authorization Documentation

Department of Management Services (DMS) rules[4] require each State agency to ensure that access to information technology (IT) resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. Specifically, DMS rules[5] provide that agency information system owners are responsible for establishing and authorizing the types of privileges and access rights appropriate to system users. Department policies and procedures[6] specified that, for FLAIR access, an Access Control Custodian (ACC) was responsible for assigning FLAIR access to additional ACCs and accounting users who required access to perform their specific job responsibilities. Additionally, Department policies and procedures[7] required business owners within the Division of Accounting and Auditing to maintain written procedures for access control to software applications and to effectively communicate the procedures to employees.

To facilitate the authorization, assignment, and review of Statewide access to the FLAIR Payroll Component, the BOSP established payroll access procedures[8] that included specific business rules for assigning access to Statewide payroll functions and directories. Our review of those procedures disclosed that the procedures for assigning access were incomplete and outdated. Specifically, we noted that the access privileges authorized for two payroll directories, DIRECTORY IRS and DIRECTORY NWS, were not included in the business rules and the list of positions authorized to assign Statewide access privileges to the FLAIR Payroll Component was inaccurate. In response to our audit inquiry, Department management indicated that the impact of staff teleworking during the COVID-19 pandemic and other competing priorities had inhibited the completion of revisions to the procedures. Further, Department management indicated that research, analysis, and documentation of all payroll functions and directories was underway and required completion prior to approval and implementation of any changes to the procedures.

Additionally, for the eight users with Statewide access to the FLAIR Payroll Component during the period March 2020 through June 2020, we evaluated the authorization for and appropriateness of access privilege changes. Our evaluation found that two user accounts were granted directory access privileges without documented approval by the user's supervisor and that the access privileges granted were not authorized by the payroll access procedures. Specifically:

- While the payroll access procedures specified that OIT staff could be granted inquiry or update access privileges to DIRECTORY VWN, an OIT user was assigned Statewide override access privileges to DIRECTORY VWN, contrary to the business rules in the procedures and without

[4] DMS Rule 60GG-2.003(1), Florida Administrative Code.

[5] DMS Rule 60GG-2-003(5)(g)6., Florida Administrative Code.

[6] *FLAIR Procedures Manual*.

[7] Department, Division of Accounting and Auditing, *System Access Control Policy*.

[8] Department, Bureau of State Payrolls, *Access Control Business Process Procedure*.

documented supervisor approval of the access privilege exception. According to OIT management, the user account was assigned to an OIT contractor whose job responsibilities included annually updating DIRECTORY VWN; however, the business rules only provided override access privileges for specified OIT users to allow them to establish access for a BOSP Payroll ACC and not for updating directories. Further, although the update only occurs annually, the override access privileges were not removed after the directory update was completed. We also noted that, while the payroll access procedures indicated that the BOSP administered access for all Statewide users, the Statewide override access privileges were granted to the OIT user by an OIT ACC, rather than a BOSP ACC, and authorization of the access granted by the OIT ACC was not documented. In response to our audit inquiry, OIT management indicated that the process to assign additional Statewide access to the FLAIR Payroll Component to OIT employees and contractors was performed as needed and that, while the process was not documented, access privileges were reviewed by OIT staff during the quarterly BOSP access review.

- For another user account, inquiry access to DIRECTORY IRS was added in error. According to Department management, the access privileges were inadvertently assigned during the process of reestablishing the user's account after the user's account was deleted because of inactivity.

Up-to-date payroll access procedures facilitate the assignment of appropriate user access privileges. Additionally, assigning access that is not explicitly authorized limits the Department's ability to demonstrate and ensure that access privileges granted to users are authorized by management and are restricted to the privileges needed for the accomplishment of the users' assigned job responsibilities.

Recommendation: We recommend that Department management promptly complete the research, analysis, and documentation of the payroll functions, update payroll access procedures accordingly, and ensure that access is granted in accordance with established procedures. We also recommend that Department management ensure that the assigned Statewide access privileges for FLAIR Payroll Component functions are reviewed and align to the updated procedures, and that access approvals are documented in Department records.

Finding 2: Background Screenings

Effective security controls include the performance of security background screenings upon hire and periodically thereafter for personnel in sensitive positions or positions of special trust. Such positions typically include IT personnel with elevated access privileges or responsibilities for the custody of sensitive IT resources. Additionally, State law[9] requires each State agency to designate positions that, because of the special trust, responsibility, or sensitive location, require background screenings. All persons and employees in such positions must undergo background screenings, including fingerprinting, as a condition of employment and continued employment.

In prior audits of the Department, most recently in our report No. 2020-095 (Finding 2), we noted that the Department had not established a comprehensive policy for the performance of background screenings of employees and contractors in positions of special trust. While Department management indicated that a Departmentwide background screening policy was in development, we noted during this audit that the Departmentwide background screening policy remained unapproved as of October 2, 2020. In response to our audit inquiry, Department management indicated that the Department continued to follow its

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

long-standing practice[10] of conducting background screenings of employees and contractors and that, although the policy had been in development for several years, it was currently being reviewed by the Department's senior leadership team.

To determine whether the Department timely conducted background screenings of contractors as a condition of providing services to the OIT, we evaluated background screening reports for 17 of the 54 OIT contractors in positions of special trust as of May 2020. The 17 OIT contractors selected for evaluation included the 7 contractors identified in our report No. 2020-095 (Finding 2) who did not have a current background screening. Our examination of Department records disclosed that the background screenings for these 7 OIT contractors were conducted 9 to 35 days (an average of 14 days) after the start date of the contractors' current contracts. According to OIT management, the finalized background screening policy would specify the required time frame to rescreen OIT contractors, including requirements for contractors without a break in service.

A comprehensive Departmentwide background screening policy and effective procedures for background screenings would decrease the risk 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 finalize the comprehensive Departmentwide background screening policy and ensure the timely performance of background screenings of contractors in positions of special trust.

Finding 3: Periodic Review of Access Privileges

DMS rules[11] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of access privileges (user and service accounts) help ensure that only authorized users and services have access and that the access privileges provided to each account remain appropriate. An effective periodic review consists of identifying the current access privileges of system users and services and evaluating the assigned access privileges to ensure that they align with user job responsibilities or service account requirements.

Department policies and procedures[12] required a formal process for the periodic review and confirmation of user accounts, access controls, and privileges. Department policies and procedures[13] also required, at a minimum, that business unit level reviews of application access privileges be conducted quarterly and documentation of the reviews to be retained for 1 year. As part of our audit, we interviewed Department staff and management, examined periodic access review policies and procedures, and evaluated related processes. Our audit procedures disclosed that, during the period July 2019 through June 2020, the Department did not review the appropriateness of the administrative accounts used to manage the Department's network domain. In response to our audit inquiry, Department management

[10] The Department's practice, effective April 1, 2013, provided for new employees and contractors hired into positions of special trust to be screened as a condition of employment and that employees transferring to a position of special trust be screened if the date of transfer was more than 6 months since the employee's last screening.

[11] DMS Rule 60GG-2.003(1)(a)6., Florida Administrative Code.

[12] Department, Division of Information Systems, Administrative Policies and Procedures No. 4-03, *Information Technology Security Policy*.

[13] Department, Division of Information Systems, Administrative Policies and Procedures No. 4-05, *Application Access Control Policy*.

indicated that due to staffing changes, the responsible OIT area was unaware of the periodic review requirements.

Periodic reviews of administrative accounts help ensure that the access privileges provided to user and service accounts remain appropriate.

Recommendation: We recommend that Department management ensure that periodic reviews of administrative accounts on the Department's network domain are conducted and documented in accordance with established policies and procedures.

Finding 4: Security Controls – Physical Access, Logical Access, User Authentication, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to physical access, logical access, user authentication, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of FLAIR data and other Department IT resources. 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 access, logical access, user authentication, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of FLAIR data and other Department IT resources may be compromised. Similar findings were communicated to Department management in connection with prior audits of the Department, most recently in connection with our report Nos. 2020-095 and 2020-056.

Recommendation: We recommend that Department management improve certain security controls related to physical access, logical access, user authentication, and logging and monitoring 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 findings included in our report No. 2020-095 and, as applicable to the scope of this audit, Finding 6 in our report No. 2020-056.

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 information technology (IT) operational audit from April 2020 through September 2020 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 significant Department of Financial Services (Department) IT controls applicable to financial reporting and Florida Accounting Information Resource Subsystem (FLAIR) and other selected Departmentwide IT controls during the period July 2019 through June 2020 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's 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. 2020-095 and Finding 6 in audit report No. 2020-056, as related to the Department's network domain.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we identified internal controls significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[14] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

[14] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by Department Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that all components of internal control were significant to our audit objectives. The associated underlying principles significant to our objectives included:

- Management commitment to integrity and ethical values.
- Management establishment of an organizational structure, assignment of responsibility, and delegation of authority to achieve the Department's goals and objectives.
- Management evaluation of employee performance and holding individuals accountable for their internal control responsibilities.
- Management establishment of clear objectives to enable the identification of risks and define risk tolerances.
- Management consideration of the potential for fraud.
- Management design of control activities to achieve the Department's objectives and respond to risks.
- Management design of controls over information technology.
- Management establishment of policies and procedures to implement internal control activities.
- Management use of relevant and quality information to achieve the Department's objectives.
- Management communication of information internally necessary to achieve the Department's objectives.
- Management activities to monitor the Department's internal control system and evaluate the results.

- Management remediation of identified internal control deficiencies on a timely basis.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; 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 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 and evaluating the IT systems and related significant 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:

- Reviewed applicable laws, rules, Department policies and procedures, and other guidelines, and interviewed Department personnel to obtain an understanding of selected significant IT business process application controls and IT general controls applicable to financial reporting and to FLAIR.
- Obtained an understanding of Department processes for approving, assigning, reviewing, and deactivating access to the FLAIR Central Accounting Component (CAC) and Payroll Component Statewide functions, including processes for ensuring an appropriate separation of incompatible duties; logical access controls for privileged users responsible for FLAIR and the underlying infrastructure and network domain; the paths and processes for authenticating to FLAIR and related systems; management and operational processes for conducting background screenings of staff and contractors employed in positions of special trust; logging and monitoring controls for system activity; physical access controls to protect Department data and IT resources; and the strategic IT planning process, including the status of Florida Planning, Accounting, and Ledger Management (PALM) project funding, planned system architecture, project oversight, and implementation schedule.
- Examined the FLAIR program change requests and work orders completed during the period July 2019 through April 2020 to determine whether the change requests or work orders significantly affected the preparation of the Statewide financial statements.

- Evaluated the interface controls related to the design and development of the Web-based application, Statewide Adjustments Management system, that is to provide State agencies the ability to submit financial adjustments online after year-end closing, and observed on July 28, 2020, data upload and interface edits of adjustment data.
- Evaluated logical access controls, including policies, procedures, and processes, for assigning, periodically reviewing, and deactivating user accounts for FLAIR CAC and Payroll Component, and the administrative-level user and service accounts for the Department's network. Specifically, we evaluated:
    - Department procedures and examined Department records to determine whether periodic reviews were performed to evaluate the appropriateness of user access privileges for FLAIR CAC and Payroll Component, and the appropriateness of administrative-level access to the Department's network.
    - The appropriateness of access for the seven FLAIR CAC users with access privilege changes during the months of March and April 2020.
    - The appropriateness of access for the eight users with Statewide access privileges to the FLAIR Payroll Component with access privilege changes during the period March 2020 through June 2020.
    - The timeliness of FLAIR CAC access privilege deactivations for the 13 Department employees with FLAIR CAC access who separated from Department employment during the period July 2019 through April 2020 and the 2 employees who had a position change during the months of March and April 2020.
    - The timeliness of FLAIR Payroll Component access privilege deactivations for the four former Department employees and one suspended employee with Statewide access privileges to the FLAIR Payroll Component during the period July 2019 through April 2020.
    - The appropriateness of the 24 administrative user accounts and the 24 administrative service accounts as of June 9, 2020, with membership in the *Enterprise Admins, Domain Admins, Schema Admins*, or *Administrators* security groups.
- Evaluated the adequacy of user identification and authentication controls for the FLAIR Departmental Accounting Component (DAC), CAC, Payroll Component, Wdesk, and the Department's network.
- Examined Departmentwide and Office of Information Technology (OIT) background screening policies and procedures regarding the performance of background screenings for employees and contractors in positions of special trust and evaluated Department records for 17 of the 54 contractors providing services to the OIT as of May 2020 to assess the timeliness of background screenings performed.
- Evaluated the appropriateness of physical access controls for the Department's Data Center and the OIT-secured areas, including the adequacy of policies, procedures, and processes established to protect Department IT resources and data. Specifically, we:
    - Observed on June 18, 2020, the Department's physical access control processes established for the Department's Data Center and the OIT-secured areas to determine whether access to IT resources was appropriately restricted.
    - Evaluated the appropriateness of physical access privileges for the 78 active key cards assigned access as of May 5, 2020, to the Data Center and the OIT-secured areas.
    - Examined Department records to determine the adequacy of the quarterly access reviews of physical access privileges to the Data Center and the OIT-secured areas for July 2019 through April 2020.

- Evaluated the adequacy of selected logging and monitoring controls.
- 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

February 19, 2021

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) and Selected Information Technology Controls.*

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

Sincerely,

Jimmy Patronis
Chief Financial Officer

JP/DC
Enclosure

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

DEPARTMENT OF FINANCIAL SERVICES RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding No. 1: Access Authorization Documentation

Department procedures for assigning Statewide access privileges to the FLAIR Payroll Component need improvement.

Recommendation: We recommend that Department management promptly complete the research, analysis, and documentation of the payroll functions, update payroll access procedures accordingly, and ensure that access is granted in accordance with established procedures. We also recommend that Department management ensure that the assigned Statewide access privileges for FLAIR Payroll Component functions are reviewed and align to the updated procedures, and that access approvals are documented in Department records.

Response: The Department concurs. The Division of Accounting & Auditing is in the process of establishing payroll functionality to positions in updated payroll access procedures. Department management will establish a process monitoring and reviewing to ensure that access is properly approved and documented.

The Office of Information Technology (OIT) is working to update the procedures related to access control for OIT workers related to Payroll functions. OIT will continue to work with BOSP in completing the access reviews timely.

Expected Completion Date for Corrective Action: July 1, 2021

Finding No. 2: Background Screenings

As similarly noted in prior audit reports, most recently in our report No. 2020-095, the Department had not established a comprehensive policy for the performance of background screenings of employees and contractors in positions of special trust. Additionally, background screening processes for contractors continue to need improvement to ensure that all contractors are screened prior to the start of contracted work.

Recommendation: We again recommend that Department management finalize the comprehensive Departmentwide background screening policy and ensure the timely performance of background screenings of contractors in positions of special trust.

Response: The Department concurs. 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.

OIT is continuing efforts to assure the process for screening and rescreening timely prior to onboarding and rescreened as recommended in the DFS draft policy. OIT has made the necessary changes to internal procedures to follow the proposed Department-wide background screening policy.

Expected Completion Date for Corrective Action: December 31, 2021

Finding No. 3: Periodic Review of Access Privileges

The Department did not conduct periodic access reviews of the administrative accounts on the Department's network domain.

Recommendation: We recommend that Department management ensure that periodic reviews of administrative accounts on the Department's network domain are conducted and documented in accordance with established policies and procedures.

Response: The Department concurs. OIT implemented corrective action to address the concerns regarding access reviews of administrative accounts related to the network domain. The OIT will continue to evaluate the processand, where appropriate, implement additional controls.

Expected Completion Date for Corrective Action: June 30, 2021

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

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

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

Response: The Department concurs. We are continuing to improve overall processes and timeliness on our physical security and user authentication processes. OIT is continuing to define the operational guides for logging and monitoring controls and reports.

Expected Completion Date for Corrective Action: June 30, 2021