STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2024-138
February 2024

DEPARTMENT OF FINANCIAL SERVICES

Florida Accounting Information Resource Subsystem (FLAIR) and Selected Information Technology General 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 Arthur Wahl, CPA, CISA, and the audit was supervised by Brenda Shiner, 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) and Selected Information Technology General 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) general controls. The audit also included a follow-up on the findings included in our report No. 2023-097. Our audit disclosed the following:

Finding 1: Department change management controls continue to need improvement to ensure that all FLAIR program changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the FLAIR production environment, and are managed by, and do not bypass, the Department's change management process.

Finding 2: FLAIR Central Accounting Component and Payroll Component Statewide access controls need improvement to ensure that access privileges are appropriately restricted.

Finding 3: Certain security controls related to logical access, user authentication, and configuration management continue to need improvement to ensure the confidentiality, integrity, and availability of FLAIR data and 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 Annual Comprehensive Financial Report (ACFR) 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, accounts payable, grants, projects, and assets. DAC provides State agency management with a budgetary check mechanism. The Statewide Financial Statements Subsystem of DAC and Workiva are used to assist and support the Department, Division of Accounting and Auditing, in publishing the State's ACFR. State agencies are the primary users of DAC.

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

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

- The Central Accounting Component (CAC), which maintains the State'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 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 created the Florida Planning, Accounting, and Ledger Management (Florida PALM) project to replace FLAIR and the cash management and accounting management components of the Cash Management Subsystem (CMS)[3] with a cloud-hosted enterprise resource planning financial management solution designed to modernize the State's financial management processes and system. Beginning with the CMS implementation (CMS Wave) in July 2021, this multi-year project was to transition FLAIR and CMS functions, as well as additional functionality, to Florida PALM using defined project waves, with production support commencing upon implementation of initial functionality. The CMS Wave transitioned the functions related to the management of bank cash, participant invested cash, and Treasury investments from the CMS to Florida PALM.

As of December 2022, the remediation and stabilization of the CMS Wave and the independent accounting and financial audit of the Department, Division of the Treasury, and its cash management transactions in Florida PALM, was completed. Additionally, following an assessment of options to replace the FLAIR Information Warehouse, the Florida PALM project was updated to include a separate data warehouse and business intelligence reporting solution that would retain historical FLAIR Information Warehouse data and Florida PALM CMS, Financials, and Payroll data.

In January 2023, the Florida PALM project timeline and implementation approach was updated, including a go-live date of January 2026 that combines the prior separate waves of Financials, Payroll, and Data Warehouse into one implementation that will build on the capabilities deployed during the CMS Wave. In May 2023, validation and finalization of the Florida PALM business requirements was completed and work began on the design of interfaces with MyFloridaMarketPlace, the Legislative Appropriations System/Planning and Budgeting Subsystem, People First, and other third-party systems. In November 2023, the official build process for the Financials and Payroll implementation began.

An Executive Steering Committee, together with the Florida PALM Project Sponsor and Project Director, are responsible for Florida PALM project governance. The Executive Steering Committee consists of 17 members representing multiple State agencies. In February 2022, the Department formed the Florida

[3] The CMS included 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 replaced eight of these applications, excluding Archive, SPIA, and CD.

PALM Advisory Council comprised of 16 FLAIR users, State agency technical staff who maintain systems that integrate with FLAIR, and State agency finance and accounting or budget directors. The Florida PALM Advisory Council is responsible for assisting the Executive Steering Committee and the Florida PALM Project Sponsor and Project Director by identifying potential solutions for future Florida PALM wave implementations.

Until Florida PALM is fully implemented, FLAIR remains the State's accounting system and, along with selected Department information technology (IT) general controls, was the subject of this audit.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management Controls

Effective change management controls are intended to ensure that all program and related changes (e.g., database changes) are properly authorized, tested, and approved for implementation into the production environment. Effective change management controls also include reconciling and reviewing all system changes implemented into the production environment for approval and appropriateness. Controls over the modification of programs, including review of before and after images of program code prior to implementation, help ensure that only approved program code changes are made within the programs.

To evaluate the appropriateness of Department change management controls for FLAIR program and related changes (program changes) implemented into the FLAIR production environment, we reviewed Department change management policies and procedures, interviewed Department personnel responsible for FLAIR change management processes, and examined change management records for FLAIR program changes implemented into the production environment. Our audit procedures found that, as of June 21, 2023, while the Department had established a reconciliation process to ensure that FLAIR program changes implemented into the production environment were appropriately authorized, tested, and approved for production, documentation of the reconciliations of FLAIR Payroll Component (Payroll) COBOL program changes were not retained. Additionally, contrary to an appropriate separation of duties, the FLAIR Payroll COBOL program change reconciliations were performed by OIT personnel responsible for both implementing and programming FLAIR Payroll COBOL program changes. In response to our audit inquiry, Department management indicated that, because only a few FLAIR Payroll COBOL program changes were implemented into production, the Department had not increased the number of personnel responsible for performing the reconciliations to ensure an independent review.

To further evaluate the appropriateness of FLAIR change management controls, we selected for audit 17 change tickets from a listing in the Department's ticketing system of the 73 FLAIR change tickets implemented during the period July 1, 2022, through June 21, 2023. For each of the 17 change tickets, we requested from the Department documentation evidencing that the program changes associated with the change tickets were properly authorized by OIT management, tested and the program code reviewed by OIT personnel independent of the OIT programmer, tested by users, approved for implementation into the production environment, and implemented into the production environment by someone other than the personnel who made or approved the changes. As similarly noted in prior audits of the Department,

most recently in our report No. 2023-097 (Finding 1), we found that neither the ticketing system nor Departmental Project Request (DPR) System[4] records included:

- An implementation approval signature on the four Move Request forms evidencing approval to implement the 17 program changes associated with 1 change ticket. In response to our audit inquiry, Department management indicated that the designated approver had retired without documenting their implementation approval on the four Move Request forms.
- A completed Analyst Checklist evidencing program code review for the changes included in 4 change tickets. According to Department management, completed Analyst Checklists for the program changes associated with 2 change tickets could not be located, a program code review was not performed for the changes included in another change ticket, and, due to oversight, an Analyst Checklist was not completed for the program change associated with the fourth change ticket.
- The signature on a Move Request form evidencing that 3 program changes associated with 1 change ticket were implemented into the production environment by an individual other than the programmer. In response to our audit inquiry, Department management indicated that the implementor of the program change neglected to sign the form.
- The Analyst Checklists for 2 change tickets indicated that the program code reviews for the changes included in the tickets were performed by the programmer of the changes and not independent OIT personnel. According to Department management, while an independent program code review was performed for the 2 program changes, the programmer signed the Analyst Checklists instead of the reviewer by mistake.

Without an independent and effective reconciliation process that ensures that all implemented FLAIR program changes are recorded in the ticketing system and accurate and complete change management records, the Department has limited assurance that all FLAIR program changes are appropriately authorized, tested, approved, and implemented into the production environment by the appropriate individual. The absence of approval records and independent program code reviews prior to implementation into the production environment increases the risk that unauthorized FLAIR program changes may be implemented into the FLAIR production environment.

Recommendation: We recommend that Department management ensure that Department records evidence through reconciliations that all FLAIR Payroll COBOL program changes are managed by, and do not bypass, the Department's change management process. Also, we again recommend that Department management improve change management controls to ensure that Department records evidence that FLAIR program changes are appropriately authorized, tested, independently reviewed, approved for production, and implemented into the production environment by the appropriate personnel.

Finding 2: Appropriateness of FLAIR Access Privileges

Effective access controls include measures that limit a user's access privileges to only those functions necessary to perform their assigned responsibilities and promote an appropriate separation of duties. Department of Management Services (DMS) rules[5] require each agency to ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties.

[4] The Department uses the DPR System to record (track) change management activities.

[5] DMS Rule 60GG-2.003(1)(d)2. and 3., Florida Administrative Code.

To facilitate the authorization, assignment, and review of Statewide access to FLAIR Payroll, the Bureau of State Payrolls (BOSP) established payroll access procedures[6] that included specific business rules for assigning access to Statewide payroll functions and directories (access privileges). Our evaluation of Statewide access to FLAIR Payroll and CAC as of May 31, 2023, found that seven users had inappropriate access. Specifically, our evaluation of 22 of the 37 FLAIR Payroll users with Statewide access found that 6 users were assigned access privileges that were not commensurate with the users' assigned job responsibilities. Additionally, our evaluation of 25 of the 151 FLAIR CAC users found that one user had inappropriate update access privileges to update tax and vendor information. In response to our audit inquiry, Department management indicated that the business rules for assigning Statewide access to FLAIR Payroll had been updated as of December 2022; however, the Department did not review and update the users' Statewide access to FLAIR Payroll based on the new business rules. Department management also indicated that the inappropriate access privileges for the one FLAIR CAC user were inadvertently not updated when the employee changed positions and, subsequent to our audit inquiry, their inappropriate access was removed.

The existence of inappropriate or unnecessary user access privileges and assigning access privileges to functions that are inappropriate or not required for the user's job responsibilities increases the risk of unauthorized modification, loss, or disclosure of FLAIR data.

Recommendation: We recommend that Department management limit Statewide access to FLAIR Payroll and CAC access privileges to only those access privileges that are appropriate and necessary for the users' assigned responsibilities.

Finding 3: Security Controls – Logical Access, 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 logical access, 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 FLAIR data and Department IT resources. However, we have notified appropriate Department management of the five findings in the three areas needing improvement.

Without appropriate security controls related to logical access, user authentication, and configuration management, the risk is increased that the confidentiality, integrity, and availability of FLAIR data and 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 No. 2023-097.

Recommendation: We again recommend that Department management improve certain security controls related to logical access, user authentication, and configuration management.

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

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. 2023-097.

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 June 2023 through November 2023 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, the Florida Accounting Information Resource Subsystem (FLAIR), and other significant Departmentwide IT controls during the period July 2022 through June 2023 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives 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 audit report No. 2023-097.
- 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 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, personnel, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, 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 the Department's organizational structure, statutory requirements, operational processes, and FLAIR components, consisting of the Departmental Accounting Component (DAC), the Central Accounting Component (CAC), and the Payroll Component (Payroll).
- Obtained an understanding of Department processes for approving, assigning, reviewing, and deactivating access to FLAIR CAC and Payroll and related databases, including processes for ensuring an appropriate separation of incompatible duties; logical access controls for the Department network domain and Workiva; the paths and processes for authenticating to the Department network domain, FLAIR components and related CAC and Payroll databases, and Workiva; Department configuration management processes related to patches and updates for servers; logging and monitoring controls for security activities for the Department network domain and Workiva; physical access controls to protect Department data and IT resources; processes for requesting, authorizing, testing, approving, implementing, and reconciling FLAIR program changes; the strategic IT planning process, including the status of the Florida Planning, Accounting, and Ledger Management (Florida PALM) project, planned system architecture, project oversight, and implementation schedule; and the Workiva adjustment process and enhancements for lease processing and subscription-based IT arrangements.
- Evaluated logical access controls, including policies, procedures, and processes, for assigning, periodically reviewing, and disabling user accounts for FLAIR CAC and Payroll Statewide access, FLAIR CAC and Payroll databases, and Department network domain administrative-level user and service accounts. Specifically, we evaluated:
    - Department procedures and examined Department records to determine whether periodic reviews of access privileges were performed to evaluate the appropriateness of access privileges for Department network domain administrative-level user and service accounts, FLAIR CAC and Payroll Statewide user accounts, and FLAIR CAC and Payroll database accounts.
    - The appropriateness of access privileges for 25 of the 151 active FLAIR CAC user accounts as of May 31, 2023.
    - The appropriateness of FLAIR CAC and Payroll database access privileges for the ten accounts as of July 5, 2023, assigned direct database access through security system group membership and the four administrator accounts as of July 6, 2023, assigned administrative-level database access through the database management system security.

- The appropriateness of access privileges for 22 of the 37 active Payroll users with Statewide access privileges as of May 31, 2023.
- The appropriateness of the eight administrative-level user accounts and the nine administrative-level service accounts as of June 28, 2023, for the Department network domain.
- The appropriateness of interactive log on capabilities for the nine administrative-level service accounts as of June 28, 2023, for the Department network domain.
- The timeliness of disabling FLAIR CAC and Payroll Statewide account access for the 12 Department employees with FLAIR CAC access privileges and the 4 Department employees with Payroll Statewide access privileges who separated from Department employment during the period July 2022 through May 2023.

- Evaluated the configuration settings as of July 5, 2023, for preventing unauthorized updates to the three FLAIR CAC and Payroll databases.
- Interviewed Department personnel and examined Department policies, procedures, and processes for FLAIR change management, including program change reconciliation processes and program code reviews. Specifically, we examined 17 of the 73 FLAIR change tickets implemented during the period July 1, 2022, through June 21, 2023, as documented in the Department's ticketing system, to determine whether the FLAIR program and related changes were appropriately authorized, tested, approved, and implemented into the production environment.
- Evaluated the adequacy of selected logging and monitoring controls.
- Evaluated the appropriateness of physical access controls for the Department's Data Center and other Office of Information Technology (OIT)-secured areas, including the adequacy of policies, procedures, and processes established to protect Department IT resources and data. Specifically, we:
  - Observed physical access controls to the Data Center and other OIT-secured areas as of August 22, 2023.
  - Evaluated the appropriateness of physical access privileges to the Data Center and other OIT-secured areas assigned to the 46 active keycards as of May 31, 2023.
  - Examined Department records to determine the adequacy of the quarterly access reviews completed in October 2022 and July 2023 of physical access privileges to the Data Center and other OIT-secured areas.
- Evaluated the adequacy of user identification and authentication controls for FLAIR DAC, CAC, and Payroll end-user access, FLAIR CAC and Payroll databases, and the Department's network domain.
- Evaluated the adequacy of configuration management policies, procedures, and processes for ensuring that server operating systems are supported and current. Specifically, we evaluated whether the operating system for the 16 Department-managed domain controllers and FLAIR-related production servers were supported and timely patched as of July 31, 2023.
- Evaluated the adequacy of interface controls related to the enhancements for lease reporting and subscription-based IT arrangements for the State's Annual Comprehensive Financial Report. Specifically, we observed data input controls, including edits and validations, and access and authentication controls as of September 11, 2023.
- 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

CHIEF FINANCIAL OFFICER
JIMMY PATRONIS
STATE OF FLORIDA

February 23, 2024

Sherrill F. Norman, CPA
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 General Controls*.

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

Sincerely,

Jimmy Patronis
Chief Financial Officer

JP/dc
Enclosure

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
200 E. Gaines Street • Tallahassee, Florida 32399-0312 • Tel. 850-413-3112 • Fax 850-413-4973
AFFIRMATIVE ACTION • EQUAL OPPORTUNITY EMPLOYER

2023 Florida Accounting Information Resource Subsystem (FLAIR) Information Technology Operational Audit

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Finding 1: Change Management Controls

Department change management controls continue to need improvement to ensure that all FLAIR program changes are appropriately authorized, tested, reviewed, and approved prior to implementation into the FLAIR production environment, and are managed by, and do not bypass, the Department's change management process.

Recommendation: We recommend that Department management ensure that Department records evidence through reconciliations that all FLAIR Payroll COBOL program changes are managed by, and do not bypass, the Department's change management process. Also, we again recommend that Department management improve change management controls to ensure that Department records evidence that FLAIR program changes are appropriately authorized, tested, independently reviewed, approved for production, and implemented into the production environment by the appropriate personnel.

Response: OIT Nancy Anderson: OIT Concurs, the FLAIR Payroll Bureau Chief and Business Analyst Manager have been granted access to the COBOL change report and are reviewing the report daily to ensure COBOL program changes are managed by the Department's change management process. We will improve change management controls to ensure FLAIR records evidence that program changes have been appropriately authorized, tested, independently reviewed, approved for production, and implemented into the production environment by the appropriate personnel.

Expected Completion Date for Corrective Action: 3/29/24

Finding 2: Appropriateness of FLAIR Access Privileges

FLAIR Central Accounting Component and Payroll Component Statewide access controls need improvement to ensure that access privileges are appropriately restricted.

Recommendation: We recommend that Department management limit Statewide access to FLAIR Payroll and CAC access privileges to only those access privileges that are appropriate and necessary for the users' assigned responsibilities.

Response: A&A Renee Hermeling: The Bureau of State Payrolls updated the business rules governing PYRL Statewide access in December 2022. At that time, six employees who were previously approved for access for use in daily job duties were reevaluated. It was determined that these employees/positions could obtain needed information in another way or no longer needed this access. A full reconciliation of the updated business rules and the current access was not

completed until 2023. This reconciliation has now occurred, and all identified employees have had the access removed.

One PYRL user and one CAC user were found to have unnecessary access. In both cases, the employee moved to another position within the Division. The access was retained to help continue completing work until vacant positions could be filled and new staff trained on the needed processes. In the case of the CAC user, the business rules were updated to reflect approval of the temporary access.

Our business rules have been further reviewed and refined during the fall of 2023 to standardize the process of updating and approving changes to the business rules. This should ensure that changes are made timely, and all access aligns with the current business rules.

Expected Completion Date for Corrective Action: 12/31/23

Finding 3: Security Controls – Logical Access, User Authentication, and Configuration Management

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

Recommendation: We again recommend that Department management improve certain security controls related to logical access, user authentication, and configuration management.

Response: OIT Stephen McKeough: Office of Information Technology, Stephen McKeough: The Office of Information Technology agrees to improve certain security controls related to logical access, user authentication, and configuration management.

Expected Completion Date for Corrective Action: 6/30/24