STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-022
September 2018

DEPARTMENT OF CHILDREN AND FAMILIES

Florida Online Recipient Integrated Data Access (FLORIDA) System

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Children and Families

The Department of Children and Families is established by Section 20.19, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, Mike Carroll served as Department Secretary.

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Hilda 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 CHILDREN AND FAMILIES

Florida Online Recipient Integrated Data Access (FLORIDA) System

SUMMARY

This operational audit of the Department of Children and Families (Department) focused on evaluating selected information technology (IT) controls applicable to the Florida Online Recipient Integrated Data Access (FLORIDA) System and included a follow-up on the findings included in our report No. 2017-009. Our audit disclosed the following:

Application Controls

Finding 1: The Department did not timely review and process numerous data exchange responses, increasing the risk that benefits may not be paid timely or accurately. Similar findings were noted in prior audits, most recently in report No. 2017-009.

Change Management Controls

Finding 2: The Department's change management controls need improvement to ensure that FLORIDA System calculation and reason code table changes follow the Department's established change management processes and changes are properly authorized, tested, and approved for implementation.

Finding 3: Certain Department change management procedures contained outdated information and the Department had not established some necessary change management procedures.

Security Controls

Finding 4: Documentation supporting authorization of access privileges to the FLORIDA System and the Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) for some employees was missing, incomplete, or incorrect. Similar findings were noted in prior audits, most recently in report No. 2017-009.

Finding 5: The Department did not conduct comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS. Similar findings were noted in prior audits, most recently in report No. 2017-009.

Finding 6: Some Department users had inappropriate access privileges to FLORIDA System resources, increasing the risk that unauthorized modification, loss, or disclosure of FLORIDA System IT resources may occur.

Finding 7: Certain security controls related to the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access for the FLORIDA System and the AMS, and related IT resources, continue to need improvement to ensure the confidentiality, integrity, and availability of the FLORIDA System and the AMS data and related IT resources.

BACKGROUND

State law[1] requires the Department of Children and Families (Department) to work in partnership with local communities to protect the vulnerable, promote strong and economically self-sufficient families, and advance personal and family recovery and resiliency. The Economic Self-Sufficiency (ESS) Program Office within the Department is responsible for public assistance eligibility determinations.[2] The public assistance programs for which the ESS Program Office determines eligibility include the Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF) Program, Medicaid Program, and Refugee Assistance Program.

The ESS Program Office utilizes the Florida Online Recipient Integrated Data Access (FLORIDA) System to assist in public assistance program eligibility determinations and benefit issuance. The Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) is a Web front-end application to the FLORIDA System mainframe that functions as a case management portal for Department staff. The client registration and application entry processes are completed within the AMS for electronic applications and loaded into the FLORIDA System, while paper applications and other public assistance processes not covered in the AMS are completed in the FLORIDA System.

FINDINGS AND RECOMMENDATIONS

APPLICATION CONTROLS

Finding 1: Data Exchange Responses

Electronic information is shared between the Department and other agencies using data exchanges. The Department performs data exchanges to comply with Federal Income and Eligibility Verification System regulations. Federal regulations[3] require State agencies to review and compare the information obtained from each data exchange against information contained in the case record to determine whether the data exchange information affects the applicant's or the recipient's eligibility or the amount of assistance. Department policy[4] provides that data exchange responses (the results of requested data exchanges) that are considered verified upon receipt by the Department must be reviewed and processed within 10 calendar days and all other responses must be reviewed and processed within 45 calendar days.

In our prior audits of the FLORIDA System, most recently in our report No. 2017-009, we noted that the Department had numerous data exchange responses that were not timely reviewed and processed. Our current review of the data exchange reports indicated that there continued to be numerous data exchange responses that the Department had not timely reviewed and processed. As of November 29, 2017, there were 650,131 (of which 523,331 were responses that were verified upon receipt) overdue data exchange responses.

[1] Section 20.19, Florida Statutes.

[2] Department Rule 65A-1.203, Florida Administrative Code.

[3] Title 45, Section 205.56(a)(1)(i), Code of Federal Regulations.

[4] *ACCESS Florida Program Policy Manual.*

As similarly noted in our report No. 2018-189, Finding Number 2017-035, effective September 26, 2016, the Department implemented a change to the FLORIDA System to purge all unreviewed data exchange responses that had been outstanding for 181 days or more. This change continued to purge unreviewed data exchange responses monthly until January 9, 2017, when the Department ceased the purging of data exchange responses. The failure to retain all documentation could affect eligibility determinations and impairs the Department's ability to demonstrate compliance with the Federal data exchange requirements.

In response to our audit inquiry, Department management stated that the number of overdue data exchange responses was due, in large part, to the volume of data exchange responses received compared to the number of staff available to process the responses. Additionally, Department management indicated that the responses to be reviewed and processed were dependent on the priority of the data exchange responses based on the type of data exchange and that many data exchange responses were not being reviewed and processed due to their low priority.

The risk that eligible individuals may not timely receive benefits and ineligible individuals may receive benefits is increased when data exchange responses are deleted or are not timely reviewed and processed.

Recommendation: We again recommend that Department management improve controls to ensure that data exchange responses are reviewed and processed within the time frames established by Department policy. We also recommend that the Department retain all data exchange responses necessary to demonstrate compliance with applicable Federal requirements.

CHANGE MANAGEMENT CONTROLS

Finding 2: Calculation and Reason Code Table Changes

Effective change management controls are intended to ensure that all modifications to IT resources are properly authorized, tested, and approved for implementation. The effectiveness of ensuring that only approved application and data changes, including table changes, are implemented is enhanced when the changes that have been moved into the production environment are reviewed for appropriateness. In addition, Agency for State Technology (AST) rules[5] require agencies to establish a configuration change control process to manage modifications to existing IT resources.

Although the Department had a change management process in place to ensure that program and table changes were appropriately authorized, tested, and approved before being implemented into the production environment, Department staff did not always use ClearQuest, the Department's approved change management ticketing system, when making FLORIDA System calculation and reason code table changes. Our review of the 37 FLORIDA System calculation and reason code table changes related to the standard quarterly Federally required changes with an effective date during the period October 1, 2016, through January 1, 2018, disclosed that 32 of the 37 FLORIDA System calculation and reason code table changes were implemented into the production environment but not documented in

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

ClearQuest. Also, Department management had not established a process to reconcile all changes implemented into the production environment to the authorized changes documented in ClearQuest.

We also found that the Department's change management process needs enhancement related to the standard quarterly Federally required changes. The ESS Office of Program Policy[6] provided memoranda to the Business Analyst describing the Federal policy changes to the public assistance programs managed in the FLORIDA System. The Business Analyst analyzed the memoranda information and prepared spreadsheets showing the FLORIDA System calculation and reason code table changes necessary to comply with the public assistance program policy changes. Once the changes were completed by programming staff, the Business Analyst performed user acceptance testing and approved the changes without review of the spreadsheets or user testing by the ESS Office of Program Policy to ensure that the Business Analyst appropriately interpreted the policy changes requested by the ESS Office of Program Policy.

A process for verifying that all application and data changes implemented into the production environment, including FLORIDA System calculation and reason code table changes are made in accordance with the Department's established change management processes provides additional assurance that FLORIDA System calculation and reason code table changes moved into the production environment have been appropriately authorized, tested, and approved for implementation. Reconciling all changes implemented into the production environment to the authorized changes documented in ClearQuest helps identify changes that bypassed the change management processes. Additionally, enhancing the change management process to include a review and approval or testing by the ESS Office of Program Policy provides additional assurance that the requested policy changes have been appropriately interpreted.

Recommendation: We recommend that Department management ensure that all application and data changes implemented into the production environment, including FLORIDA System calculation and reason code table changes, follow the Department's established change management processes to ensure that the changes are properly authorized, tested, and approved for implementation. Additionally, we recommend that Department management revise the change management process to include the reconciliation of changes implemented into production to the authorized changes documented in ClearQuest. We also recommend that the change management process for policy changes be enhanced to include review and approval by the ESS Office of Program Policy prior to implementation of the changes.

Finding 3: Change Management Procedures

Effective change management controls include documented change management procedures that reasonably assure that changes to application functionality are authorized and appropriate, and that unauthorized changes are detected and promptly reported. Reviews of applicable State and Federal regulations in conjunction with reviews of Department procedures would help ensure Department procedures reflect current State, Federal, and industry standards.

[6] The ESS Office of Program Policy is responsible for public assistance policy within the ESS Program Office.

Our audit procedures related to the Florida System calculation and reason code table changes disclosed that certain Department change management procedures contained outdated information and some necessary change management procedures had not been established. Specifically, we found that:

- The ESS Office of Program Policy had not established written procedures for documenting the receipt of changes in Federal program requirements and for processing the related FLORIDA System table changes. For example, Department procedures should address the processes for identifying, documenting, reconciling, and monitoring relevant changes to ensure that the FLORIDA System tables are timely and accurately updated by the Department's Office of Information Technology Services (OITS).
- The OITS established a *Mass Change Instructions* document which provided detailed steps for making changes to the FLORIDA System calculation and reason code tables and the related mass change processes. However, at the time of our review, this document had not been updated since the mid-1990s and did not reflect current processes. For example, the *Mass Change Instructions* did not reflect the use of ClearQuest to record change activities and did not specify which change activity steps should be recorded or how they should be recorded. Subsequent to our audit inquiry, Department staff updated the *Mass Change Instructions* on February 9, 2018.

Documented and updated change management procedures help ensure that system changes made by employees are commensurate with Federal requirements and management's direction.

Recommendation: We recommend that Department management continue efforts to ensure that applicable change management procedures are documented and kept up-to-date.

SECURITY CONTROLS

Finding 4: Access Authorization Documentation

Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. Additionally, access authorization documentation should be maintained in an appropriate manner to facilitate the complete and accurate assignment of user access privileges.

We requested the FLORIDA System Individual Security Information Forms (access authorization forms) for 40 of the 3,363 users who had both FLORIDA System and AMS user access privileges as of December 27, 2017. We reviewed the access authorization forms provided to determine whether the forms indicated both FLORIDA System and AMS user access. We found that, as of December 27, 2017, some access authorization forms were not available, were incomplete, or did not support the user access privileges granted. Specifically, we found that:

- Department management was unable to provide the access authorization forms for 3 of the 40 users with FLORIDA System and AMS access privileges. However, Department management provided other access authorization documentation authorizing FLORIDA System access privileges for 1 of the 3 users.
- The access authorization forms on file did not match the current level of access assigned to certain users. Specifically:
    - Of the 38 FLORIDA System users for which the Department provided access authorization forms or other access authorization documentation, the security profile information authorized for 20 users did not match the access privileges assigned.

- Of the 37 AMS users for which the Department had access authorization forms, the security profile information authorized for 27 users did not match the access privileges assigned. For 21 of the 27 AMS users, access privileges to AMS were not authorized because the access authorization form did not include a field for selecting AMS access and AMS access was not specified on the forms (i.e., not identified in "Other" access form field). For the remaining 6 AMS users, while the access authorization form included a field for selecting AMS access, the field was not marked.

- Supervisor approval of the access privileges granted was not evident for 6 of the 38 users for whom the Department provided access authorization documentation.

In response to our audit inquiry, Department management stated that access authorization forms for some employees may not have been available because access requests may have been submitted by a supervisor in an e-mail; however, Department staff were unable to provide such documentation.

Missing, incomplete, or access authorization forms that do not support the user access privileges granted limit the Department's ability to demonstrate and ensure that the user access privileges granted to employees are authorized by management and are appropriate for the accomplishment of assigned job duties. Similar findings were noted in prior audits, most recently in our report No. 2017-009.

Recommendation: We again recommend that Department management improve controls to ensure that access authorization forms are retained, complete, and commensurate with management's direction and that access privileges are only granted as indicated on the access authorization forms.

Finding 5: Periodic Review of User Access Privileges

AST rules[7] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. The Department's *Standard Operating Procedure SOP S-12: Data Security Administration* (*SOP S-12*) requires business unit level reviews of application access privileges to be conducted annually at a minimum to ensure that the access privileges of users are consistent with the roles and responsibilities the users require to perform their assigned duties.

Our audit procedures disclosed that, contrary to *SOP S-12*, the Department had not conducted comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS. In response to our audit inquiry, Department management stated that a periodic review of all users would require additional staffing as the effort would be extensive.

Without the periodic review of FLORIDA System and AMS user access privileges, management's assurance that user access privileges were authorized and appropriate is limited and the Department cannot demonstrate compliance with AST rules. Similar findings were noted in prior audits, most recently in our report No. 2017-009.

Recommendation: We again recommend that Department management conduct a comprehensive periodic review of access privileges for the FLORIDA System and the AMS and establish procedures to ensure that the reviews are performed annually as required by *SOP S-12*.

[7] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

Finding 6: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. In addition, AST rules[8] require all users be granted access to agency IT resources based on the principles of least privilege and a need to know determination.

Our review of Department records for nine users who had user accounts with update access privileges to FLORIDA System calculation tables as of January 26, 2018, disclosed the following:

- Seven user access accounts were assigned to three Department employees (two Department security administrators and one staff member working in the OITS testing section), one Department contractor (programmer), and three non-Department State employees (security administrators for other agencies) who did not have a business purpose for updating the FLORIDA System calculation tables.
- Two user access accounts were assigned to users (a Department employee working as a systems project analyst and a Department contractor working as a systems programmer) with a valid business purpose for updating the FLORIDA System calculation tables. However, the profile granted to these two users provided them excessive access privileges that allowed them to perform functions as end-users, contrary to an appropriate separation of duties.

The existence of inappropriate and unnecessary user access privileges increases the risk that unauthorized modification, loss, or disclosure of FLORIDA System IT resources may occur.

Recommendation: We recommend that Department management limit user access privileges to the FLORIDA System to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

Finding 7: Security Controls – Protection of Confidential and Exempt Data, Logging and Monitoring, User Authentication, and Logical Access

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 the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access for the FLORIDA System and the AMS and related Department IT resources need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Similar findings related to the protection of confidential and exempt data were previously communicated to Department management, most recently in connection with our report No. 2017-009.

Without adequate security controls related to the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access the risk is increased that the confidentiality, integrity, and availability of the FLORIDA System and the AMS data and related IT resources may be compromised.

Recommendation: We recommend that Department management improve security controls related to the protection of confidential and exempt data, logging and monitoring, user

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

authentication, and logical access to ensure the confidentiality, integrity, and availability of FLORIDA System and AMS data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report No. 2017-009.

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 September 2017 through April 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 applicable to the FLORIDA System and the AMS during the period July 2017 through April 2018 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing, and output and selected application-level general controls applicable to the FLORIDA System and the AMS that related to the deficiencies disclosed in our report No. 2017-009. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2017-009.
- 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 Department documentation to obtain an understanding of:
  - The data and business process flows for the FLORIDA System including key sources of data input, interfaces, key application transactions and processes, and key types of application data output.
  - The data exchange processing controls.
  - User account management processes for authorizing, creating, modifying, and revoking access to the FLORIDA System and the AMS.
- Evaluated selected FLORIDA System transaction data processing controls for data exchanges. Specifically, we evaluated controls related to how exceptions are investigated and resubmitted for processing and to the new processes implemented for unprocessed data exchange responses.
- Evaluated selected FLORIDA System transaction data error processing controls. Specifically, we:
  - Evaluated documentation related to FLORIDA System processing for eligibility determinations and benefit calculations to determine whether processing errors were identified, logged, and resolved.
  - Examined 25 new Disaster SNAP, TANF, and Refugee cash cases with unique case sequence numbers approved during the period July 1, 2017, through January 31, 2018, to assess whether the FLORIDA System accurately calculated benefit payments according to program rules.
  - Evaluated SNAP documentation for February 2018 to determine if applicable SNAP cases were closed as required to prevent future SNAP payments.
  - Evaluated processing controls designed to prevent duplicate benefit payments in the FLORIDA System.
  - Examined the cases associated with 25 of 108 payees identified as having more than one approved SNAP case or case sequences during the period July 1, 2017, through

October 31, 2017, to assess the effectiveness of FLORIDA System controls in preventing duplicate SNAP benefits.

- Evaluated logging and monitoring controls related to the use of FLORIDA System override transactions.

- Evaluated selected FLORIDA System and AMS access controls. Specifically, we:
  - Examined Department procedures, to obtain an understanding of and determine whether management-approved FLORIDA System and the AMS security administration procedures were documented.
  - Evaluated FLORIDA System and AMS access authorization processes and examined the authorization of access privileges for 40 of the 3,363 unique Economic and Self-Sufficiency user accounts with access to the FLORIDA System and the AMS as of December 27, 2017.
  - Evaluated Department access controls to obtain an understanding of how the Department limited access privileges to individuals with a valid business purpose (least privilege).
  - Assessed the appropriateness of access privileges for 40 of the 3,363 unique Economic and Self-Sufficiency user accounts with access to the FLORIDA System and the AMS as of December 27, 2017.
  - Examined Department access controls to obtain an understanding of the Department's process for disabling or removing inactive accounts or accounts for individuals who have transferred or separated from Department employment.
  - Examined Department records to assess whether system owners periodically reviewed access privileges to the FLORIDA System and the AMS to ensure continued appropriateness.
- Evaluated selected access controls for restricting, logging, and monitoring access privileges to the FLORIDA System database. Specifically, we:
  - Evaluated Department administrative access to the FLORIDA System database and examined the one user account with UPDATE or ALTER access privileges to the datasets containing the FLORIDA System production tables and database logs as of November 21, 2017, and November 22, 2017, respectively, to evaluate the appropriateness of the access privileges.
  - Evaluated logging and monitoring controls related to the use of sensitive or privileged accounts that directly access the FLORIDA System database.
- Evaluated the appropriateness of FLORIDA System and AMS application and FLORIDA System database identification and authentication controls as of November 14, 2017.
- Evaluated the sufficiency of Department controls to protect confidential data related to the FLORIDA System and the AMS. Specifically, we inspected:
  - Department records to evaluate the controls over the protection of confidential data as of February 27, 2018, and February 28, 2018.
  - Department records to evaluate the controls over the protection of social security numbers held by the Department as of October 27, 2017.
- Evaluated selected program and data change management controls related to the FLORIDA System. Specifically, we evaluated:
  - Department procedures for program change management related to the FLORIDA System to assess whether the procedures are designed to reasonably assure that FLORIDA System changes are authorized and that unauthorized changes are detected and reported promptly.

- Department mass change procedures for implementing changes to the FLORIDA System tables, including the calculation and reason code tables, to assess whether the tables are timely and accurately changed.
- The effectiveness of change controls for 37 FLORIDA System calculation and reason code table changes related to the standard quarterly Federal changes with a Federal effective date during the period October 1, 2016, through January 1, 2018.
- The appropriateness of update access privileges to FLORIDA System calculation tables for the nine unique users who had update access privileges to the FLORIDA System calculation tables as of January 26, 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

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Secretary

August 28, 2018

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

Dear Ms. Norman:

Thank you for the opportunity to respond to your August 2 list of preliminary and tentative audit findings and recommendations on the information technology operational audit of the Florida Online Recipient Integrated Data Access (FLORIDA) System.

This letter is the Department and Children and Families' response. Should you have any questions, please contact Joe Vastola, Chief Information Officer at (850) 320-9132.

Application Controls

Finding No. 1: Data Exchange Responses - The department did not timely review and process numerous data exchange responses, increasing the risk that benefits may not be paid timely or accurately. Similar findings were noted in prior audits, most recently in report No. 2017-009.

Recommendation: We again recommend that department management improve controls to ensure that data exchange responses are reviewed and processed within the time frames established by department policy. We also recommend that the department retain all data exchange responses necessary to demonstrate compliance with applicable federal requirements.

Office of Economic Self-Sufficiency (ESS) Response: The department concurs with this finding. The department has improved controls through the implementation of the Data Exchange (DE) system controls and automation enhancement on September 26, 2016, which prevents eligibility staff from authorizing benefits prior to processing un-reviewed DEs. Since implementation, staff have processed 11,191,206 DEs and, in turn, reduced the backlog to 625,232 overdue DEs as of August 14, 2018. Overdue DEs

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

have been reduced from 1.6 million on April 10, 2015[1], to 1 million on May 18, 2016[2], to 650,131 on November 29, 2017 (current finding), representing a decrease of 59 percent. As of August 14, 2018, the number of overdue DEs is 625,232, which is an overall decrease of 61 percent from April 2015 to August 2018.

Effective January 9, 2017, the department retains all data exchange responses necessary to demonstrate compliance with applicable federal requirements.

The department has made significant gains in its effort to reduce overdue DEs and ensure DEs are reviewed and processed within the established timeframes. The department will continue its efforts to make further improvements.

Change Management Controls

Finding No. 2: Calculation and Reason Code Table Changes - The department's change management controls need improvement to ensure that FLORIDA System calculation and reason code table changes follow the department's established change management processes and changes are properly authorized, tested, and approved for implementation.

Recommendation: We recommend that department management ensure that all application and data changes implemented into the production environment, including FLORIDA System calculation and reason code table changes, follow the department's established change management processes to ensure that the changes are properly authorized, tested, and approved for implementation. Additionally, we recommend that department management revise the change management process to include the reconciliation of changes implemented into production to the authorized changes documented in ClearQuest. We also recommend that the change management process for policy changes be enhanced to include review and approval by the ESS Office of Program Policy prior to implementation of the changes.

Office of Economic Self-Sufficiency Response: Currently, ClearQuest does not support the ability for the ESS Program Office to sign-off officially on the table change request. Therefore, a process has been developed by which the ESS Program Office sends a table change request form to the Office of Information Technology Services (OITS), who, in turn, creates the change request. Once the table changes have been completed, OITS verifies and then sends them to the ESS Program Office for final

[1] Florida Auditor General Report No. 2016-007
[2] Florida Auditor General Report No. 2017-009

verification in acceptance before moving them to production. The ESS Program Office also has final review of the production change as well.

Office of Information Technology Services Response: The department agrees that calculation and code tables were not documented and tracked in the department's change management tool (ClearQuest). The original intent of relaxing requirements for tracking changes to these tables was to provide more responsive service to the ESS Program Office by allowing requests to be made via email. However, it was determined that email was an ineffective tool for tracking calculation and code table changes. The department reverted to requiring all changes to be tracked and managed in ClearQuest starting March 2018. Currently, the department meets the recommendation for this finding.

Finding No. 3: Change Management Procedures - Certain department change management procedures contained outdated information and the department had not established some necessary change management procedures.

Recommendation: We recommend that department management continue efforts to ensure that applicable change management procedures are documented and kept up-to-date.

Office of Information Technology Services Response: The department concurs with this finding. The OITS will work with the ESS Program Office to establish written procedures for documenting the receipt of changes for federal program requirements and the tracking of those changes affecting FLORIDA System table changes. Projected resolution date for this finding is July 1, 2019.

Security Controls

Finding No. 4: Access Authorization Documentation - Documentation supporting authorization of access privileges to the FLORIDA System and the Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) for some employees was missing, incomplete, or incorrect. Similar findings were noted in prior audits, most recently in report No. 2017-009.

Recommendation: We again recommend that department management improve controls to ensure that access authorization forms are retained, complete, and commensurate with management's direction and that access privileges are only granted as indicated on the access authorization forms.

Office of Information Technology Services Response: The department concurs that there have been instances discovered in which ACCESS Security Forms are incomplete or missing. The OITS will continue to work with Headquarters and Regional Security Officers to reinforce compliance with security form storage and archival requirements. Currently, the department is evaluating the feasibility of automating ACCESS Security Forms in order to more effectively access, track, and update systems access authorizations. Projected resolution date for this finding is July 1, 2019.

Finding No. 5: Periodic Review of User Access Privileges - The department did not conduct comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS. Similar findings were noted in prior audits, most recently in report No. 2017-009.

Recommendation: We again recommend that department management conduct a comprehensive periodic review of access privileges for the FLORIDA System and the AMS and establish procedures to ensure that the reviews are performed annually as required by SOP S-12.

Office of Information Technology Services Response: The department concurs that periodic reviews of user access privileges should be required and enforced and, to that end, has undertaken the development of an automated system (Security Audit System) that will allow managers and supervisors statewide the ability to review and approve access privileges. This system is scheduled to be deployed as a pilot in the DCF Suncoast Region by September 2018, and pending the outcome of the pilot program, will be deployed for statewide use in FY 2018-2019.

Finding No. 6: Appropriateness of Access Privileges - Some department users had inappropriate access privileges to FLORIDA System resources, increasing the risk that unauthorized modification, loss, or disclosure of FLORIDA System IT resources may occur.

Recommendation: We recommend that department management limit user access privileges to the FLORIDA System to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

Office of Information Technology Services Response: The department concurs with this finding. The assignment of access privileges was designed to allow flexibility in users' roles so that workload impact on units could be mitigated by as needed assignment of roles. The department will review access privileges of users and limit access privileges where possible to ensure compliance with least privilege principles. This will include limiting an HQ security officer's profile to modify table changes only to

specific individuals who will be performing this function. Projected resolution date for this finding is July 1, 2019.

Finding No. 7: Security Controls – Protection of Confidential and Exempt Data, Logging and Monitoring, User Authentication, and Logical Access – Certain security controls related to the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access for the FLORIDA System and the AMS, and related IT resources, continue to need improvement to ensure the confidentiality, integrity, and availability of the FLORIDA System and the AMS data and related IT resources.

Recommendation: We recommend that department management improve security controls related to the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access to ensure the confidentiality, integrity, and availability of FLORIDA System and AMS data and related IT resources.

Office of Information Technology Services Response: The department concurs with this finding. The department received funding in FY 2017-2018 and FY 2018 – 2019 to implement tools and programs to comply with the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standard for Exchanges (MARS-E) 2.0 Security and Privacy Controls based on the NIST 800-53 Rev 4 standards. In July 2018, the department implemented a Security Information and Event Monitoring (SIEM) tool that allows wide-ranging auditing, reporting, and data analytics functions for logging and monitoring of systems activities, including user access to applications, networks, and IT resources. In FY 2018-2019, the department will greatly expand its MARS-E 2.0 compliance efforts by implementing a variety of security tools and programs as well as new and updated policies and procedures governing security and privacy controls.

Sincerely,

Mike Carroll
Secretary