STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-007
August 2015

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 of Children and Families who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, Michael Carroll served as Department Secretary.

The team leader was Debra Clark, CPA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF CHILDREN AND FAMILIES

Florida Online Recipient Integrated Data Access (FLORIDA) System

SUMMARY

The Florida Online Recipient Integrated Data Access (FLORIDA) System and the Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) are maintained by the Office of Information Technology Services within the Department of Children and Families (Department). The FLORIDA System is a Statewide system used by the Economic Self-Sufficiency (ESS) Program Office within the Department to assist in public assistance program eligibility determination and benefit issuance. Public assistance programs include Food Assistance, Temporary Cash Assistance, Medicaid, and Refugee Assistance. The AMS is used to track assignments and the progress of work items within the FLORIDA System.

This operational audit focused on evaluating selected information technology (IT) controls applicable to the FLORIDA System and the AMS and included a follow-up on the findings included in our report No. 2014-196. As summarized below, the audit disclosed areas in which improvements in the FLORIDA System and the AMS controls and operational processes were needed.

Application Controls

Finding 1: The Department had numerous data exchange responses that had not been reviewed and processed and were overdue. The untimely review and processing increases the risk that ineligible individuals may receive benefits.

Security Controls

Finding 2: Documentation of authorization for both the FLORIDA System and the AMS access privileges for some employees was missing, incomplete, or incorrect. Also, the Department did not have documented procedures to be used for the security administration of the AMS.

Finding 3: The Department had not conducted comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS.

Finding 4: Certain Department security controls related to passwords and data transmission, logging and review, and protection of confidential and exempt data needed improvement.

BACKGROUND

The Department of Children and Families (Department) was created pursuant to Section 20.19, Florida Statutes, which states, in part, that the Department is 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. Also, Section 409.031, Florida Statutes, designates the Department as the State agency responsible for the administration of social service funds under Title XX of the Social Security Act. According to Department Rules 65A-1.203(1) and (2), Florida Administrative Code, the Economic Self-Sufficiency (ESS) Program Office is the entity within the Department responsible for

public assistance eligibility determination, and public assistance programs include Food Assistance, Temporary Cash Assistance, Medicaid, and Refugee Assistance.

The ESS Program Office uses the Florida Online Recipient Integrated Data Access (FLORIDA) System and the Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) to assist in the processing of applicants, eligibility determination, and benefit issuance for public assistance programs. The FLORIDA System and the AMS are composed of application modules that function to collect client information relating to income and assets. However, the FLORIDA System also evaluates the client information to determine the eligibility of a family or individual and calculates and generates public assistance benefits. The client registration and application entry process is completed within the AMS for electronic applications and interfaced to the FLORIDA System, while paper applications and other public assistance processes not covered in the AMS are completed in the FLORIDA System. The FLORIDA System and the AMS are maintained by the Department's Office of Information Technology Services and are housed and operated at the Northwood Shared Resource Center (NSRC).

FINDINGS AND RECOMMENDATIONS

APPLICATION CONTROLS

Finding 1: Data Exchanges

Data exchange is the sharing of electronic information between the Department and other agencies. The Department performs data exchanges to comply with the Federal Income and Eligibility Verification System regulations. The Department's *ACCESS Florida Program Policy Manual* provided 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; all other responses must be reviewed and processed within 45 calendar days.

The ESS Program Office incorporated both daily and monthly data exchange reports to track the number of data exchange responses requiring processing. The data exchange reports were available on a Web-accessible Data and Reports System. Our review of the data exchange reports indicated that there were numerous data exchange responses that had not been reviewed and processed and were overdue. As of April 10, 2015, there were over 1.6 million (approximately 674,000 of which were responses that were verified upon receipt) overdue data exchange responses. The data exchange reports included responses that were at least 1 day over the 10- and 45-calendar-day review and processing requirements established in the *ACCESS Florida Program Policy Manual* and did not provide the number of days overdue for each response. As a result, we were unable to determine the full extent to which the responses were overdue.

In response to our audit inquiry, Department management stated that data exchange 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 lack of a timely review and processing of data exchange

responses increases the risk that ineligible individuals may receive benefits, as similarly noted in prior audits of the Department, most recently our report No. 2014-196.

Recommendation: The Department should improve controls to ensure that data exchange responses are reviewed and processed within the time frames established by Department policy.

SECURITY CONTROLS

Finding 2: Documentation of User Access Authorizations

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. The Department's *FLORIDA Security Guide* documented the procedures and forms, including security profiles and security levels, to be used for the security administration of the FLORIDA System. However, the Department did not have documented procedures to be used for the security administration of the AMS.

We requested access authorization forms for 40 employees who had FLORIDA System user access privileges as well as AMS user access privileges as of March 30, 2015. Our audit procedures disclosed that, as of March 30, 2015, some access authorization forms were missing, incomplete, or incorrect with regard to the user access privileges granted. Specifically, we noted that:

FLORIDA System

- The access authorization form for 1 employee was missing and could not be provided by the Department.
- The access authorization forms for 16 employees did not include appropriate security profile and security level information.
- The security profile and security level information authorized on the access authorization forms for 3 employees did not match the user access privileges assigned.

AMS

- The access authorization forms for 33 employees were missing and could not be provided by the Department.
- The access authorization forms for 3 employees did not include the appropriate security profile and security level information.

Missing, incomplete, or incorrect access authorization forms increase the risk that the Department's ability may be limited in ensuring that user access privileges granted to employees are authorized by management and are appropriate for the accomplishment of assigned job duties. A similar finding was noted in prior audits of the Department, most recently our report No. 2014-196. Additionally, the lack of documented security administration procedures for the AMS increases the risk that AMS access privileges granted to employees may not be commensurate with management's direction.

Recommendation: The Department should improve controls to ensure that access authorization forms are retained, complete, and commensurate with management's direction and that applicable security administration procedures are documented.

Finding 3: Periodic Review of User Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic review of user access privileges helps to 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.

Contrary to *SOP S-12*, our audit procedures disclosed that the Department had not conducted comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS. Without the periodic review of the appropriateness of access privileges, the risk is increased that inappropriate access privileges may exist and not be timely detected or corrected. A similar finding was noted in prior audits of the Department, most recently our report No. 2014-196.

Recommendation: The Department should conduct comprehensive periodic reviews of access privileges for the FLORIDA System and the AMS.

Finding 4: Security Controls - Passwords and Data Transmission, Logging and Review, and Protection of Confidential and Exempt Data

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain Department security controls related to passwords and data transmission, logging and review, and protection of confidential and exempt data for the FLORIDA System, the AMS, and related IT resources needed 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 were communicated to Department management in connection with prior audits of the Department, most recently our report No. 2014-196. Without adequate security controls related to passwords and data transmission, logging and review, and protection of confidential and exempt data, the risk is increased that the confidentiality, integrity, and availability of FLORIDA System and AMS data and related IT resources may be compromised.

Recommendation: The Department should improve security controls related to passwords and data transmission, logging and review, and protection of confidential and exempt data to

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

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 findings included in our report No. 2014-196.

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 February 2015 through March 2015 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 2014 through March 2015 and selected actions through June 3, 2015. The audit included selected business process application controls over transaction data input and processing and selected application-level general controls applicable to the FLORIDA System that related to the deficiencies disclosed in audit report No. 2014-196 and selected IT controls applicable to the AMS as related to the FLORIDA System. The audit also included selected application-level general controls related to security management. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2014-196.
- 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 ineffective or inefficient 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.
- Obtained an understanding of the IT computing platforms for the FLORIDA System and the AMS.
- Obtained an understanding of the process for authorizing access privileges for the FLORIDA System and the AMS.
- Evaluated the effectiveness of selected access controls to ensure that the authorized access privileges to the FLORIDA System and the AMS were appropriately granted. Specifically, for 40 employees who had FLORIDA System user access privileges as well as AMS user access privileges as of March 30, 2015, we reviewed access authorization forms and the access privileges granted to determine if the authorized access privileges were appropriately granted.
- Evaluated selected access controls related to the appropriateness of access privileges to the FLORIDA System and related IT resources and the comprehensive periodic reviews of user access privileges for the FLORIDA System and the AMS. Specifically, we reviewed the access privileges of 83 FLORIDA System users to determine appropriate separation of duties as of March 30, 2015. Also, we reviewed 14 users granted access privileges to FLORIDA System production datasets, operating system logs, database logs, production program, and job control language as of March 24, 2015.
- Evaluated selected application access controls related to the protection of FLORIDA System passwords and data during transmission and storage.
- Evaluated selected audit logging and monitoring capability.
- Obtained an understanding of the FLORIDA System's purpose and goals involving compliance requirements.

- Obtained an understanding of the data and business process flows for the FLORIDA System with an emphasis on the AMS and how it interacts with the FLORIDA System.
- Evaluated selected transaction data input procedures for the FLORIDA System.
- Evaluated selected transaction data input and processing procedures for the AMS.
- Evaluated the effectiveness of configuration management controls over the FLORIDA System. Specifically, we evaluated selected application configuration management procedures for the FLORIDA System and the AMS. We also reviewed 12 program change requests that were moved into the production environment between July 1, 2014, and March 25, 2015, to determine whether selected FLORIDA System and AMS program changes were appropriately authorized, documented, tested by an independent party, and approved and implemented into the production environment.
- Evaluated selected FLORIDA System procedures for the protection of confidential and exempt data.
- 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

July 29, 2015

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 June 29 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.

Enclosed is the Department of Children and Families' response. Should you have any questions, please contact Scott Stewart, Chief Information Officer, at (850) 320-9265.

Sincerely,

Mike Carroll
Secretary

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery and Resiliency

RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM

Finding No. 1: The Department had numerous data exchange responses that had not been reviewed and processed and were overdue. The untimely review and processing increases the risk that ineligible individuals may receive benefits.

Recommendation: The Department should improve controls to ensure that data exchange responses are reviewed and processed within the time frames established by Department policy.

Office of Economic Self-Sufficiency (ESS) Response: The Department concurs with this finding. The Department has made some gains in its efforts to eliminate the backlog of overdue data exchange (DE) responses from a high of over 2 million in January 2012 to over 1.6 million in April 2015, which represents a 20 percent reduction in the number of overdue DE responses. As of July 20, 2015, the Department has reduced the number of overdue DE responses to 1,469,403, which is an additional decrease of eight percent between April 2015 and July 2015. Of critical importance is that many DE responses received may be duplicates, or may have been received during the certification period, therefore requiring no action. Due to these factors, the potential impact on accuracy and the actual number of overdue DEs may be overstated. These two factors persist because of the limitations of the FLORIDA system as well as limited resources to enhance the system as necessary to stay current as policies change. Also of note is the system's reliance on manual (worker) intervention to process most DEs, which is intensified by an ever-increasing caseload and stagnant human resources over the last year. ESS is committed to, and emphasizes the importance of, timely processing DEs.

As such, the elimination of the backlog and prevention of future occurrences are now a high priority for all Department stakeholders. Through a coordinated effort between the Offices of Economic Self-Sufficiency and Information Technology Services (ITS), and Operations, the Department continues to work to improve its processes, both automated and manual, to ensure that adequate monitoring controls are in place to eliminate the backlog of overdue DE responses. The coordinated efforts include, but are not limited to, the following corrective actions to strengthen current strategies and identify new ones:

- Performance improvement meetings;
- DE analysis;
- Development of a tolerance threshold for compliance; and
- Requirement for Regional corrective action plans.

Finding No. 2: Documentation of authorization for both the FLORIDA System and the Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) access privileges for some employees was missing, incomplete, or incorrect.

Also, the Department did not have documented procedures to be used for the security administration of the AMS.

Recommendation: The Department should improve controls to ensure that access authorization forms are retained, complete and commensurate with management's direction and that applicable security administration procedures are documented.

Office of Information Technology Services Response: The Department concurs with this finding. Currently we are updating the ACCESS security guides to include information on the maintenance of the security access forms. Once the updates are completed, the guide will be distributed to all ACCESS security officers. We are also updating the FLORIDA individual request form to include requested role assignment for AMS and other ACCESS systems as well. This change will also be disseminated to security officers once completed.

Finding No. 3: The Department had not conducted comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS.

Recommendation: The Department should conduct comprehensive periodic reviews of access privileges for the FLORIDA System and the AMS.

Office of Information Technology Services Response: The Department concurs with this finding. The Department currently provides security officers with a daily file from PeopleFirst of all employees who have terminated employment with the Department. Also, there is a monthly reconciliation report that is reviewed by security officers to ensure that employees who no longer require access to the systems are immediately terminated.

The Department is in the midst of a project to update its information security operating procedures. An outcome of the project will be a DCF Access Control operating procedure that requires comprehensive periodic reviews of access privileges by the information owners.

Finding No. 4: Certain Department security controls related to passwords and data transmission, logging and review, and protection of confidential and exempt data needed improvement.

Recommendation: The Department should improve security controls related to passwords and data transmission, logging and review, and protection of confidential and exempt data 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 and continues to address and work toward correcting the issues raised.