STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-009
August 2016

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 Karen Thomas, 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

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. 2016-007. Our audit disclosed the following:

Application Controls

Finding 1: The Department had numerous data exchange responses that had not been reviewed and processed and were overdue. Untimely review and processing increases the risk that ineligible individuals may receive benefits. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

Security Controls

Finding 2: 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. In addition, the Department did not have written procedures for the security administration of the AMS, thus increasing the risk that AMS access privileges granted to employees may not be commensurate with management's direction. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

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. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

Finding 4: Certain security controls related to passwords and data transmission and protection of confidential and exempt data for the FLORIDA System, the AMS, and related IT resources continue to need improvement to ensure the confidentiality, integrity, and availability of the FLORIDA System and AMS data and related IT resources. Similar findings were previously communicated to Department management, most recently in connection with our report No. 2016-007.

BACKGROUND

The Department of Children and Families (Department) was created pursuant to State law,[1] 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. The Economic Self-Sufficiency (ESS) Program Office within the Department is responsible for public assistance eligibility determination.

[1] Section 20.19, Florida Statutes.

The Florida Online Recipient Integrated Data Access (FLORIDA) System is used by the ESS Program Office to assist in eligibility determination 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 process is 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 Exchanges

Electronic information is shared between the Department and other agencies using data exchanges. The Department performs data exchanges to comply with the Federal Income and Eligibility Verification System regulations. The Department's *ACCESS Florida Program Policy Manual* 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.

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, as of May 18, 2016, there were over 1 million overdue data exchange responses. Approximately 340,000 of these overdue responses were responses that had been verified upon receipt. The data exchange reports identified responses that were at least 1 day over the 10- and 45-calendar-day review and processing time frames established in the *ACCESS Florida Program Policy Manual* but did not provide the number of days each response was overdue. As a result, the full extent to which the responses were overdue could not be determined.

In response to our audit inquiry, Department management stated that the number of overdue data exchange responses, in large part, was due 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 many data exchange responses were not being reviewed and processed due to their low priority.

The risk that ineligible individuals may receive benefits is increased when data exchange responses are not timely reviewed and processed. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

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

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* (*Guide*) documented the procedures and forms, including security profiles, 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 both FLORIDA System and AMS user access privileges as of April 2, 2016. Our audit procedures disclosed that, as of April 2, 2016, some access authorization forms were missing, incomplete, or incorrect with regard to the user access privileges granted. Specifically, we noted that:

- FLORIDA System access authorization forms for 6 employees were missing and could not be provided by the Department.
- FLORIDA System access authorization forms for 14 employees did not include appropriate security profile information.
- The security profile information authorized on the FLORIDA System access authorization forms for 3 employees did not match the user access privileges assigned.
- AMS access authorization forms for 35 employees were missing and could not be provided by the Department.
- AMS access authorization forms for 2 employees did not include the appropriate security profile information.

In response to our audit inquiry, Department management stated that authorization forms for some employees may not have been available because of the user's longevity and other authorization forms may not have been available because of the turnover of Department security officers.

Missing, incomplete, or incorrect access authorization forms limit the Department's ability to demonstrate and ensure that 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. 2016-007. Additionally, as similarly noted in our report No. 2016-007, 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: We recommend that Department management 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) rules[2] required agency information owners to 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.

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 there were no detailed processes in place to ensure reviews of user access privileges were adequately performed.

Without the periodic review of the FLORIDA System and AMS user access privileges, management's assurance that user access privileges were authorized and appropriate is limited. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

Recommendation: We 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*.

Finding 4: Security Controls - Passwords and Data Transmission 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 security controls related to passwords and data transmission 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 previously communicated to Department management, most recently in connection with our report No. 2016-007.

Without adequate security controls related to passwords and data transmission and protection of confidential and exempt data, the risk is increased that the confidentiality, integrity, and availability of the FLORIDA System and AMS data and related IT resources may be compromised.

[2] AEIT Rule 71A-1.007(2), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records, property, administrative authority, and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST. On June 5, 2016, Chapters 71A-1 and 71A-2, Florida Administrative Code, were repealed. The AST adopted Rules 74-2.001 through 74-2.006, Florida Administrative Code, effective March 16, 2016, establishing the Florida Cybersecurity Standards. AST Rule 74-2.003(1)(a)6., Florida Administrative Code, requires periodic reviews of access privileges based on system categorization or assessed risk.

Recommendation: We recommend that Department management improve security controls related to passwords and data transmission and protection of confidential and exempt data to ensure the confidentiality, integrity, and availability of the FLORIDA System and AMS data and related IT resources.

PRIOR AUDIT FOLLOW-UP

The Department had not taken corrective actions for the findings included in our report No. 2016-007.

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 April 2016 through May 2016 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 2015 through May 2016. 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. 2016-007. 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. 2016-007.
- 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.
- Obtained an understanding of the FLORIDA System's background, including the FLORIDA System's purpose and goals involving financial, operations, and compliance requirements.
- Obtained an understanding of FLORIDA System data and business process flows, including key sources of data input, including interfaces; key application transactions and processes; and key types of application data output related to the FLORIDA System.
- Evaluated the effectiveness of selected FLORIDA System business process application controls related to data input. Specifically, as of May 18, 2016, we reviewed 12 selected online edits built into the FLORIDA System to determine if the edits were in place and operating effectively.
- Evaluated selected FLORIDA System business process application controls related to data processing and output and interfaces.
- Obtained an understanding of the Department's user account management processes for authorizing, creating, modifying, and revoking access to the FLORIDA System and the AMS.
- Evaluated the effectiveness of selected FLORIDA System and AMS application access authorization controls. Specifically, we reviewed selected access authorization controls for 40 users with active FLORIDA System and AMS access privileges as of April 2, 2016.
- Evaluated selected FLORIDA System and AMS application access controls related to review procedures for access appropriateness.
- Evaluated selected FLORIDA System and AMS controls for passwords and data transmission and the protection of confidential and exempt data.
- Obtained an understanding of the Department's procedures for logging, retaining, and monitoring network logs.
- Evaluated selected network logging controls.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.

- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Secretary

August 16, 2016

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 July 14 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 Joe Vastola, Chief Information Officer, at (850) 320-9132.

Sincerely,

Mike Carroll
Secretary

Enclosure

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: 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

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. Untimely review and processing increases the risk that ineligible individuals may receive benefits. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

Recommendation: We recommend that department management 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 and continues its efforts to eliminate the overdue data exchange (DE) backlog and to improve system controls to ensure DEs are reviewed and processed within the established time frames. Overdue DEs have been reduced from 1.6 million on April 10, 2015 to 1 million on May 18, 2016, representing a decrease of 38 percent. As of July 29, 2016, the number of overdue DEs has been further reduced to 859,540, which is an overall decrease of 46 percent from April 2015 to July 2016.

The department formed a statewide DE workgroup of key stakeholders from the Offices of Economic Self-Sufficiency and Information Technology Services and Operations. The workgroup's efforts are focused on the following:

- DE Backlog Clean Up – Each region is committed to eliminating their share of the backlog by September 15, 2016.

- System Controls and Automation Implementation – In order to prevent future backlogs and ensure DEs are processed within timeframes, the system controls and automation will prevent eligibility staff from authorizing benefits prior to processing un-reviewed DEs and are scheduled for implementation on September 26, 2016.

Finding No. 2: 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. In addition, the department did not have written procedures for the security administration of the AMS, thus increasing the risk that AMS access privileges granted to employees may not be commensurate with management's direction. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

Recommendation: We recommend that department management 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 FLORIDA Security Guide is being updated to emphasize controls related to the preservation and storage of the Florida Individual Security Information Form (CF 113). The instructions added to the guide will match those already existing in the department's operating procedure SOP S-12. Once completed, regional security officers will have refresher training to ensure the procedures are understood and followed.

Additionally, existing language in the department's ACCESS Management System (AMS) Work Management Guide make it clear that AMS profiles and access are created by and dependent upon the profiles set in FLORIDA/RACF. At the time AMS was released into production, access to the system was generated and determined based on the user's FLORIDA access. As such, Florida Individual Security Information Forms completed prior to the AMS rollout will only reflect the user's FLORIDA System access. Forms complete after the rollout, and a subsequent revision to the form to include reference to AMS, should have the user's AMS access and role identified. Activities undertaken to satisfy Finding No. 3 will address and resolve inconsistencies related to AMS access documentation.

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. Similar findings were noted in prior audits, most recently in our report No. 2016-007.

Recommendation: We 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 continues to provide security officers with a daily file from People First of all staff terminating employment. Also, a monthly reconciliation report is provided to and reviewed by the department's regional security officers. This reconciliation report helps identify staff no longer requiring access to the FLORIDA or ACCESS Management System and have their privileges terminated immediately.

The department is currently working with management from the operations, technology, and security areas to revise its information security operating procedures. Included in these procedures will be processes to ensure compliance with SOP S-12.

Finding No. 4: Certain security controls related to passwords and data transmission and protection of confidential and exempt data for the FLORIDA System, the AMS, and related IT resources, continue to need improvement to ensure the confidentiality, integrity, and availability of the FLORIDA System and AMS data and related IT

resources. Similar findings were previously communicated to department management, most recently in connection with our report No. 2016-007.

Recommendation: We recommend that department management improve security controls related to passwords and data transmission and protection of confidential and exempt data to ensure the confidentiality, integrity, and availability of the FLORIDA System and AMS data and related IT resources.

Office of Information Technology Services Response: The department agrees with the finding in principle. An initial evaluation of the finding and prospective solutions indicate remedies would be costly and require substantive application changes and the purchase of additional network equipment. The department is actively evaluating the relevant business needs, cost, and implication of the changes needed and researching potential alternate solutions that may resolve this finding.