REPORT NO. 2014-196
JUNE 2014

DEPARTMENT OF CHILDREN AND FAMILIES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

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, the following individuals served as Department Secretary:

Esther Jacobo, Interim	From July 19, 2013
David Wilkins	Through July 18, 2013

The audit team leader was Russell DeHennis 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 can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CHILDREN AND FAMILIES

Florida Online Recipient Integrated Data Access (FLORIDA) System

SUMMARY

The Florida Online Recipient Integrated Data Access (FLORIDA) System is a Statewide system maintained by the Office of Information Technology Services within the Department of Children and Families (Department). The Public Assistance (PA) Component within the FLORIDA System is used by the Economic Self-Sufficiency (ESS) Program Office in public assistance program eligibility determination and benefit issuance.

Our audit focused on evaluating selected information technology (IT) controls applicable to the FLORIDA System. We also determined the status of corrective actions regarding prior audit findings of the Department that were included in our report No. 2013-005.

Our audit disclosed areas in which enhancements in FLORIDA System controls and operational processes were needed. Many of these findings were also disclosed in our prior IT audits of the FLORIDA System. The results of our audit are summarized below:

APPLICATION CONTROLS

Finding No. 1: As similarly noted in prior audits of the Department, FLORIDA System edits designed to prevent employees from performing incompatible functions could be circumvented in certain instances.

Finding No. 2: As similarly noted in prior audits of the Department, the Department had numerous unprocessed overdue data exchange responses. When not processed timely, there is an increased risk that ineligible individuals may receive benefits.

SECURITY CONTROLS

Finding No. 3: As similarly noted in prior audits of the Department, documentation of authorization for the FLORIDA System PA Component access privileges of some employees was missing or incomplete.

Finding No. 4: As similarly noted in prior audits of the Department, the IT resource access privileges of some Department and Northwood Shared Resource Center (NSRC) employees, former employees, and contractors were inappropriate.

Finding No. 5: The Department did not perform comprehensive periodic reviews of the appropriateness of access privileges.

Finding No. 6: As similarly noted in prior audits of the Department, certain Department security controls related to passwords and system data needed improvement.

OTHER GENERAL CONTROLS

Finding No. 7: The Department was unable to provide documentation that some appropriate approvals had occurred prior to the implementation of program changes into the production environment.

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 ensure the safety, well-being, and self-sufficiency of the people served. 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 Rule 65A-1.203, Florida Administrative Code, the Economic Self-Sufficiency (ESS) Program Office is the entity within the Department responsible for public assistance eligibility determination. Public assistance programs include the Temporary Assistance for Needy Families, Supplemental Nutrition Assistance, and Medical Assistance Programs. The ESS Program Office utilizes the Florida Online Recipient Integrated Data Access (FLORIDA) System to assist in eligibility determination and benefit issuance for public assistance programs.

The FLORIDA System PA Component is composed of numerous application modules that function to collect and evaluate client information, such as income and asset information; determine eligibility of a family or individual; and calculate and generate public assistance benefits. The FLORIDA System is maintained by the Department's Office of Information Technology Services and is housed and operated at the Northwood Shared Resource Center (NSRC).

FINDINGS AND RECOMMENDATIONS

Application Controls

Finding No. 1: Separation of Duties

An appropriate separation of duties includes a division of roles and responsibilities that ensures that employees are performing only those duties stipulated for their respective jobs and positions. The FLORIDA System security profiles are used to assist in promoting an appropriate separation of duties between incompatible functions related to all aspects of managing a recipient's case, referred to as case management, including requesting and approving auxiliary benefits and fiats. In addition, for situations where an employee required multiple profiles that could possibly create a separation of duties issue, an edit of the user identification code (user ID) together with a unique identifier was implemented that would prevent a user with multiple user IDs from registering a client and authorizing benefits for that client. The edit was also in place for the request and approval of auxiliary benefit transactions that were used to provide benefits in addition to benefits calculated by the FLORIDA System and for request and approval of fiats that are special transactions that allow users to override eligibility determination and benefit calculation performed by the FLORIDA System.

For example, when a user attempts to approve a fiat for a client, the FLORIDA System checks the user's user ID and unique identifier to determine whether the same user initiated the fiat. If the user ID of the user attempting to approve the fiat is the same as the user ID that initiated the fiat, then the FLORIDA System will not allow that user to approve the fiat. If the user ID that is attempting to approve the fiat is different from the user ID that requested the fiat, then the FLORIDA System checks the unique identifier of the two user IDs to determine if the user IDs belong to the same user. If the unique identifiers are the same for the two user IDs, the system will not allow the user to approve the fiat. If a user with multiple user IDs does not have the same unique identifier recorded for each user ID, then the user could perform incompatible duties in the FLORIDA System.

Our audit disclosed that 2 users included in our test of 94 user IDs with at least two different user IDs (one with the security profile ELIGPASS and the other with the security profile CASEPAS) had the ability to circumvent the FLORIDA System edits that prevented the users from both initiating and approving a fiat because the unique identifiers assigned to at least one of the user IDs was not correct. In response to our inquiry, Department management provided documentation indicating that during the period of our audit one user had circumvented the edits in four instances. However, Department management indicated that corrections had been made to the unique identifiers of the user IDs so that they no longer had the capability to create and approve a fiat for a client. A similar finding was disclosed in prior audits of the Department, most recently our report No. 2013-005.

A lack of an appropriate separation of duties may compromise the integrity of eligibility determination and the accuracy of eligible benefit amounts within the FLORIDA System. If a single employee has the ability to perform incompatible transactions within the FLORIDA System, there is an increased risk that fraud may occur without being timely detected.

Recommendation: The Department should monitor the accuracy of unique identifiers that are recorded in security profiles of users to ensure the proper functioning of the system edits enforcing an appropriate separation of case management duties.

Finding No. 2: 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. Department policy provided that data exchange responses (the results of requested data exchanges) that are considered verified upon receipt by the Department must be processed within 10 calendar days; all other responses must be processed within 45 calendar days.

The ESS Program Office developed data exchange reports to track the number of data exchange responses requiring processing. These reports were available on a Web-accessible Data and Reports System and were refreshed every morning from FLORIDA System data. Although these online data exchange reports were available to allow ESS staff to monitor data exchange responses, the reports also indicated that there were numerous data exchange responses that had not been processed and were overdue. As of February 25, 2014, there were over 1.3 million (approximately 789,500 of which were responses that were verified upon receipt) overdue data exchange responses.

In response to audit inquiry, Department management indicated that the large volume of unprocessed overdue data exchange responses existed because of an insufficient number of staff and an increase in the number of benefit requests. When data exchange responses are not processed in a timely manner, there is an increased risk that ineligible individuals may receive benefits, as similarly noted in prior audits of the Department, most recently our report No. 2013-005.

Recommendation: The Department should implement controls for ensuring that data exchange responses are processed within the time frames established by Department policy.

Security Controls

Finding No. 3: Documentation of User Access Authorizations

Effective security controls include logical (electronic) access controls that restrict legitimate and appropriate users to the specific IT resources needed and prevent others from accessing the resources. Access controls include, among other things, the use of access authorization forms to document the access privileges that have been authorized by management to be granted to system users.

According to the *FLORIDA Security Guide*, FLORIDA System user account administration (creating, modifying, or revoking user access privileges to the FLORIDA System) is shared between regional and headquarters security officers. Regional security officers manage FLORIDA System access privileges of employees within their assigned districts. The headquarters security officer (Information Systems Security Administrator) manages security profiles

and also performs user account management for headquarters staff. According to the *FLORIDA Security Guide*, access authorization forms must be completed and submitted to regional security officers to add, modify, or revoke a FLORIDA System user account. Required information on these forms includes first and last name, action required, security profile name, and security level. Other information is required depending on the nature of the request.

Our audit disclosed instances where, as discussed below, the Department had not appropriately documented authorizations of user access privileges granted to some users, contrary to the *FLORIDA Security Guide.* A similar finding was noted in prior audits of the Department, most recently our report No. 2013-005.

We requested access authorization forms for 40 active FLORIDA System PA Component users as of December 31, 2013. For 3 of the 40 users included in our review, the Department could not provide the required authorization forms. For the remaining 37 users for which authorization forms were provided, the authorization forms of 1 user did not include security profile or security level information to indicate authorization for the security profile and security level that had been granted to the user. However, the access levels granted to the user did not appear to be inappropriate based on the user's job duties. Nevertheless, when authorizations for user access privileges are not appropriately documented, these conditions limit management's ability to ensure that user access privileges granted to employees are authorized by management and are appropriate for the accomplishment of assigned job duties.

Recommendation: The Department should enhance its FLORIDA System PA Component user account management processes by ensuring that access authorization forms are retained and complete.

Finding No. 4: Appropriateness of Access Privileges

Limiting access privileges to only what is needed in the performance of assigned job duties helps protect IT resources from unauthorized disclosure, modification, and destruction. Inappropriate access privileges within systems increase the risk of errors, fraud, misuse, or unauthorized alteration of data and IT resources. Our audit disclosed that, as of December 19, 2013, some Department and NSRC employees, former employees, and contractors had inappropriate access privileges to production datasets containing the FLORIDA System production data, operating system logs, database logs, production programs, and job control language (JCL). Specifically, we noted the following:

- Five employees and one contractor had alter (create, update, and delete) access to operating system logs that was not necessary for their job duties.
- Two former employees who had terminated employment on November 1, 2013, and November 22, 2013, retained alter access to database logs and production data, 48 and 27 days, respectively, after their termination dates, with the latter also retaining alter access to operating system logs.
- Another former employee who terminated employment on October 25, 2013, retained alter access to the production programs and JCL for 55 days after his termination date.

When inappropriate access exists as described above, there is an increased risk that unauthorized changes to production data, operating system logs, database logs, production programs, and JCL may occur, as similarly noted in prior audits of the Department, most recently our report No. 2013-005.

Recommendation: The Department should enhance security controls to ensure the appropriateness of access privileges granted to the FLORIDA System production datasets and to ensure the timely deactivation of access privileges of former employees and contractors.

Finding No. 5: Periodic Review of User Access Privileges

Periodic review of access privileges helps ensure that access privileges remain appropriate. Our audit disclosed that the Department had not conducted comprehensive periodic reviews of user access privileges for the FLORIDA System and related IT resources. Additionally, the Department had not established written procedures for periodically reviewing the access privileges of users. 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.

Recommendation: The Department should establish and follow written procedures for conducting comprehensive periodic reviews of access privileges for the FLORIDA System and related IT resources.

Finding No. 6: Security Controls - Passwords and Data Transmission

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to passwords and the transmission of Department data that 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 noted in prior audits of the Department, most recently our report No. 2013-005. Without adequate security controls related to passwords and data transmission, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

Recommendation: The Department should improve password and data transmission controls to ensure the confidentiality, integrity, and availability of data and IT resources.

Other General Controls

Finding No. 7: Program Changes to the FLORIDA System Production Environment

Effective program modification controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation. The effectiveness of program change controls is enhanced when management's expectations for the control of program changes are documented in the form of written procedures.

Although the Department had established written program change control procedures, Department staff indicated, in response to audit inquiry, that established program change procedures were not always followed. Department staff did not always document approvals of program changes prior to work beginning, code testing, and user acceptance testing (UAT). Specifically, for 40 program changes we reviewed, we noted the following:

- Thirty-nine did not have evidence of approval prior to work beginning.
- Thirty-two did not have evidence of code testing approval by Department management.
- Nine did not have evidence of UAT approval prior to program changes being moved into the production environment.

Without documentation of appropriate approvals, the risk is increased that erroneous or unauthorized changes may be moved into the production environment.

Recommendation: The Department should follow established program change procedures to ensure that all program changes are appropriately approved and documentation of the approvals is retained.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for two of the findings included in our report No. 2013-005 that were applicable to the scope of this audit. Corrective actions were not taken for six of the eight prior audit findings as described in the findings above.

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 December 2013 through March 2014 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to the FLORIDA System 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. An additional objective was to determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2013-005 that were within the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to the FLORIDA System during the period July 2013 through March 2014 and selected Department actions through April 8, 2014, including selected application level general IT controls over systems development and modification, and logical access security.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls and IT controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective IT operational policies, procedures, or practices. The focus of this IT operational 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 system and controls included within the scope of our audit, the 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 our audit; obtaining an understanding of the IT system 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our 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 our audit, we:

- Interviewed Department and NSRC personnel.
- Obtained an understanding of the Department's FLORIDA System including the computing platform and related software, purpose and goals, and the basic data and business process flows through the PA Component.
- Obtained an understanding of key FLORIDA System PA Component application and access controls, including input, processing, output, and user controls.
- Observed and evaluated the effectiveness of key application control processes and procedures, including eligibility determination and cutoff, benefit processing, and data exchange.
- Observed and evaluated the effectiveness of key FLORIDA System access control processes and procedures.
- Evaluated the effectiveness of controls over separation of duties of Department staff with access to the FLORIDA System PA Component. Specifically, we evaluated 94 of 5,050 user accounts to determine whether the access levels granted enforced an appropriate separation of duties between auxiliary benefits and fiat transaction creation and authorization.
- Evaluated the effectiveness of procedures for authorizing user access privileges and the appropriateness of the access privileges granted. Specifically, we evaluated 40 of 5,050 FLORIDA System PA Component users and all 35 unique RACF user accounts to determine whether the access authorization was documented and the profiles and security levels granted were appropriate.
- Obtained an understanding of general IT controls related to the FLORIDA System.
- Observed and evaluated key processes and procedures related to logical access controls over FLORIDA System IT resources.
- Evaluated the effectiveness of logical access controls over selected FLORIDA System IT resources. Specifically, we evaluated 120 user accounts within 18 security profiles with access to mainframe datasets to determine whether the access granted was appropriate.
- Evaluated the effectiveness of FLORIDA System password settings to evaluate the effectiveness of the settings in adequately protecting resources.
- Observed and evaluated key Department program change control processes and procedures for the FLORIDA System. Specifically, we evaluated 40 of 765 FLORIDA System program changes that were moved into the production environment between July 1, 2013, and January 29, 2014, to determine whether the program changes were adequately approved, designed, tested, and implemented.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing 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 those matters requiring corrective action.

AUTHORITY

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated May 22, 2014, the Interim Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Interim Secretary

May 22, 2014

David W. Martin, Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Auditor General Martin:

Thank you for the opportunity to respond to your April 28 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 Mark Powell, IT Audits and Compliance Manager, at (850) 320-9168.

Sincerely,

Mike Carroll
Interim Secretary

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS

DEPARTMENT OF CHILDREN AND FAMILIES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM
Information Technology (IT) Operational Audit

FINDING NO. 1: As similarly noted in prior audits of the Department, FLORIDA System edits designed to prevent employees from performing incompatible functions could be circumvented in certain instances.

RECOMMENDATION: The Department should monitor the accuracy of unique identifiers that are recorded in security profiles of users to ensure the proper functioning of the system edits enforcing an appropriate separation of case management duties.

RESPONSE: The audit identified two FLORIDA users with improperly assigned profiles. We have corrected these profiles. The Department will implement a review process by which FLORIDA user profile assignments are validated by an additional step in the assignment process.

FINDING NO. 2: As similarly noted in prior audits of the Department, the Department had numerous unprocessed overdue data exchange responses. When not processed timely, there is an increased risk that ineligible individuals may receive benefits.

RECOMMENDATION: The Department should implement controls for ensuring that data exchange responses are processed within the time frames established by Department policy.

PROGRAM OFFICE RESPONSE: Through its quality assurance efforts, the Department's Economic Self-Sufficiency (ESS) Office of Quality Management (QM) ensures Data Exchanges (DEs) are monitored at the state and local levels in accordance with Department policy to ensure they are processed timely and accurately and requires corrective action, where necessary. ESS QM has expanded monitoring efforts at the state and local level to include the following:

- Added a DE review element to the Food Assistance, TANF and Medicaid case reviews in the statewide electronic case review system (QMS) to ensure that any DEs associated with cases reviewed for these programs are processed timely and accurately.

- Added a targeted review to QMS for the following DE types that have a major impact on eligibility:
  - Child Support Enforcement Sanctions
  - Work Sanctions

1

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

FINDING NO. 3: As similarly noted in prior audits of the Department, documentation of authorization for the FLORIDA System PA Component access privileges of some employees was missing or incomplete.

RECOMMENDATION: The Department should enhance its FLORIDA System PA Component user account management processes by ensuring that access authorization forms are retained and complete.

RESPONSE: The Department has enhanced its FLORIDA System PA Component user account management process by creating a procedure for maintaining security access forms. Security officers will scan the completed access forms and store them in a secure location on the network. See SOP S-12 (10) and (11).

FINDING NO. 4: As similarly noted in prior audits of the Department, the IT resource access privileges of some Department and Northwood Shared Resource Center (NSRC) employees, former employees, and contractors were inappropriate.

RECOMMENDATION: The Department should enhance security controls to ensure the appropriateness of access privileges granted to the FLORIDA System production datasets and to ensure the timely deactivation of access privileges of former employees and contractors.

RESPONSE: The Department is working with NSRC system administrators to conduct a review of the appropriateness of access to production datasets and to develop a process to receive notification when NSRC mainframe staff, who have system access, leave the Department or change job duties.

As a compensating control, the FLORIDA system automatically revokes the Resource Access Control Facility (RACF) account for the user after 45 days of inactivity. The FLORIDA System has been modified to send a monthly Security Maintenance/User Management (SMUM/RACF) Reconciliation report to the security officers to ensure that any discrepancies between SMUM and RACF are resolved timely.

FINDING NO. 5: The Department did not perform comprehensive periodic reviews of the appropriateness of access privileges.

RECOMMENDATION: The Department should establish and follow written procedures for conducting comprehensive periodic reviews of access privileges for the FLORIDA System and related IT resources.

RESPONSE: The Department will establish written procedures for conducting comprehensive periodic reviews of access privileges for the FLORIDA System and related IT resources. The anticipated completion date is December 2014. The Office of Information Technology will work with the program areas to determine the best way to implement the periodic reviews statewide.

FINDING NO. 6: As similarly noted in prior audits of the Department, certain Department security controls related to passwords and system data needed improvement.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

RECOMMENDATION: The Department should improve password and data transmission controls to ensure the confidentiality, integrity, and availability of data and IT resources.

RESPONSE: The Department concurs with this finding and is in the process of addressing this issue.

FINDING NO. 7: The Department was unable to provide documentation that some appropriate approvals had occurred prior to the implementation of program changes into the production environment.

RECOMMENDATION: The Department should follow established program change procedures to ensure that all program changes are appropriately approved and documentation of the approvals is retained.

RESPONSE: ACCESS IT currently employs a change and production control management process for review and approval of all program system changes as defined by SOP 50-17. To correct this deficiency ACCESS IT will enforce documented approvals for all changes via its current tracking tool for authorizing work approval, code testing, and User Acceptance Testing prior to moving changes into the production environment.