REPORT NO. 2013-005
AUGUST 2012

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

Pursuant to Section 20.19(2)(a), Florida Statutes, the Secretary of the Department of Children and Families is appointed by the Governor, subject to confirmation by the Senate. David E. Wilkins served as Secretary during the period of our audit.

The audit team leader was Robert McKee, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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) 487-9175; 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 is used by the Economic Self-Sufficiency (ESS) Program Office in public assistance program eligibility determination and benefit issuance. The Child Support Enforcement Component is used by the Department of Revenue to support Child Support Enforcement Program Office activities.

Our audit of the FLORIDA System focused on evaluating selected information technology (IT) controls applicable to the FLORIDA System. We also determined the status of corrective actions regarding audit findings disclosed in our prior audit reports, including, most recently, report No. 2011-141.

As summarized below, our audit disclosed that the Department had not corrected many prior audit findings regarding IT controls applicable to the FLORIDA System:

APPLICATION CONTROLS

Finding No. 1: Contrary to Section 119.071(5)(a)2.a., Florida Statutes, the Department used certain employee social security numbers (SSNs) without specific authorization in law or without having established the imperative need to use the SSN for the performance of its duties and responsibilities as prescribed by law. This finding was also noted in prior audits of the Department, most recently our report No. 2011-141.

Finding No. 2: As similarly noted in our report No. 2010-066, FLORIDA System edits designed to prevent employees from performing incompatible case management functions could be circumvented in certain instances.

Finding No. 3: The Department had numerous unprocessed overdue data exchange responses. Similar findings were noted in prior audits of the Department, most recently our report No. 2011-167, Finding FA 10-064, and report No. 2011-141.

SECURITY CONTROLS

Finding No. 4: As similarly noted in prior audits of the Department, most recently our report No. 2011-141, documentation of authorization for the FLORIDA System PA Component access privileges of some employees was missing, incomplete, or inaccurate.

Finding No. 5: The IT resource access privileges of some mainframe technical support staff and groups exceeded what was necessary for their job duties. Similar findings were noted in prior audits of the Department, most recently our report Nos. 2010-066 and 2011-141.

Finding No. 6: As similarly noted in prior audits of the Department, most recently our report No. 2011-141, the Department did not timely deactivate the PA Component access privileges of some former employees.

Finding No. 7: Certain Department security controls related to passwords and the transmission of FLORIDA System information needed improvement. Similar findings related to passwords were noted in prior audits of the Department, most recently our report No. 2011-141.

OTHER GENERAL CONTROLS

Finding No. 8: As similarly noted in prior audits of the Department, most recently our report No. 2011-141, the Department's systems development and modification policies and procedures 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 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. A CSE Component was formerly used by the Department of Revenue to locate noncustodial parents, establish paternity, establish support obligations, and enforce support obligations when the noncustodial parent fails to make support payments or provide medical coverage as ordered by the court. However, the CSE Component was removed from the FLORIDA System in January 2012. 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: Use of SSNs

Section 119.071(4)(a), Florida Statutes, provides that all employee SSNs held by the employing agency are confidential and exempt from public inspection. Pursuant to Section 119.071(5)(a)2.a., Florida Statutes, an agency may not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless the agency is specifically authorized by law to do so, or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

As also noted in prior audits of the Department, most recently our audit report No. 2011-141, the Department collected and used certain employee SSNs in the FLORIDA System. To avoid the possibility of compromising Department information, we are not disclosing in this report the specific details of how the SSN was used. However, we have notified appropriate Department personnel of this issue.

No specific authorization existed in law for the Department to collect the SSNs of employees who used the FLORIDA System and the Department had not established the imperative need to use the SSN for the performance of its duties and responsibilities instead of another number. The use of the SSN was contrary to State law and increased the risk of improper disclosure of SSNs.

Recommendation: In the absence of establishing an imperative need for the use of the SSN, the Department should comply with State law by establishing another number to be used in the FLORIDA System rather than the SSN.

Finding No. 2: Separation of Duties

Separation of incompatible duties is fundamental to the reliability of an agency's internal controls. The Department enforced a separation of case management duties through the use of security profiles and edits in the FLORIDA System. However, our audit disclosed an instance where an edit preventing employees from performing incompatible functions, such as requesting and approving auxiliary benefits and fiats (system overrides), could be circumvented. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising Department information. However, we have notified appropriate Department personnel of the specific issue. A similar finding was disclosed in our report No. 2010-066.

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

Recommendation: The Department should take steps to minimize the likelihood that the FLORIDA System edit enforcing an appropriate separation of case management duties could be circumvented.

Finding No. 3: 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 disposed of within 45 calendar days.

The ESS Program Office developed data exchange reports to track the number of data exchanges. 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 overdue. As of January 18, 2012, there were over 2 million (approximately 929,000 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, an increase in the number of benefit requests, and duplicate data exchanges. 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. 2011-167, Finding FA 10-064, and report No. 2011-141.

Recommendation: The Department should continue to seek solutions for ensuring that data exchange responses are processed within the required time frames.

Security Controls

Finding No. 4: 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 employees contrary to the *FLORIDA Security Guide*. A similar finding was noted in prior audits of the Department, most recently our report No. 2011-141.

We requested access authorization forms for a sample of 60 of 5,337 active FLORIDA System PA Component user accounts as of December 12, 2011. For 6 of the 60 user accounts included in our sample, Department staff could not provide the authorization form. Of the 54 authorization forms on file, 3 forms lacked the security profile, the security level, or both. Additionally, access levels shown as authorized on 1 additional form did not match the access levels actually granted in the FLORIDA System. The access levels granted, however, did not appear to be excessive based on the job duties of the FLORIDA System PA Component user listed on the form. Nevertheless, these conditions limited management's ability to ensure that user access privileges granted to employees do not exceed what is necessary for the accomplishment of assigned job duties.

Recommendation: The Department should improve its FLORIDA System PA Component user account management procedures by ensuring that access authorization forms are appropriately completed, accurate, and maintained.

Finding No. 5: 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. Excessive access privileges within systems increase the risk of errors, fraud, misuse, or unauthorized alteration of data and IT resources. Our audit disclosed that some NSRC employees had unnecessary and excessive access privileges to datasets containing the FLORIDA System production database and database logs and production programs and job control language (JCL). Specifically, of 122 user accounts tested:

- Two NSRC mainframe technical support employees had access privileges to modify the FLORIDA System production database and database logs that recorded activities performed on datasets. These access privileges were unnecessary for the performance of the job duties of the two technical support staff. Under these

conditions, the risk was increased that unauthorized modifications could be made to the FLORIDA System production database or database logs, rendering the logs unreliable for use in detecting inappropriate database access. A similar finding with regard to operating system log access privileges was disclosed in our report No. 2011-141.

- Two NSRC mainframe technical support groups had ALTER (update) access privileges to datasets that contained FLORIDA System production programs and JCL. Employees within these two groups did not need update access to perform their job duties and the risk was increased of unauthorized modification or destruction of production programs and JCL. A similar finding involving a Department employee with unnecessary ALTER access to production programs and JCL was disclosed in our report No. 2010-066.

Recommendation: The Department should remove the unnecessary and excessive access privileges and review the ongoing appropriateness of all access privileges granted to the FLORIDA System production datasets to ensure that access is commensurate with the requirements of employee job duties and to ensure the reliability of the above-described FLORIDA System IT resources.

Finding No. 6: Timely Deactivation of Former Employee Access Privileges

Effective access controls include provisions for the timely deactivation of former employee access privileges to ensure that the access privileges are not misused by the former employee or others. According to the *FLORIDA Security Guide*, an employee's access privileges are to be deactivated immediately upon termination of employment with the Department or when the employee moves to a part of the Department where access to the FLORIDA System is no longer necessary. The employee's supervisor is to submit to the appropriate FLORIDA security officer a written request for the employee's access privileges to be deactivated.

As similarly noted in prior audits of the Department, most recently our report No. 2011-141, our audit disclosed that the Department did not timely deactivate the PA Component access privileges of some former employees within the ESS Program Office, increasing the risk of inappropriate activity within the FLORIDA System. For a sample of 60 of 776 former employees, who had terminated employment from the Department between April 1, 2011, and November 22, 2011, we reviewed FLORIDA System PA Component user access listings to determine whether the former employees had access to the FLORIDA System and whether their privileges were deactivated in a timely manner. Fifty-six of the 60 former employees included in our sample had access to the FLORIDA System. For 23 of the 56 former employees with user accounts, access privileges had not been timely deactivated in the FLORIDA System. Specifically, FLORIDA System access privileges for 18 of the 56 former employees remained active beyond the next business day for various time periods up to 31 days after termination. The access privileges for 5 former employees were not deactivated for various time periods from 33 to 178 days after termination. Although not timely deactivated, all of the 23 former employees' access privileges had been deactivated by the Department prior to our testing. We noted during other access authorization testing of active accounts as of December 12, 2011, that two users having active FLORIDA System accounts were terminated from the Department. Specifically:

- One former employee with an active FLORIDA System account terminated on September 2, 2011. In response to audit inquiry, Department staff deactivated this individual's account on February 1, 2012, 152 days after his date of termination. This account was not used subsequent to his termination date.
- The other former employee with an active FLORIDA System account terminated on December 31, 2009. In response to audit inquiry, Department staff deactivated this individual's account on February 7, 2012, 768 days after her date of termination. This account was not used subsequent to her termination date.

Additionally, we noted that one former employee's FLORIDA System access privileges remained active for 5 days after her date of termination. Although not timely deactivated, this former employee's FLORIDA System access

privileges had been deactivated by the Department prior to our testing. Department transaction logs indicated the access privileges of the former employee had been used on April 4, 2011, subsequent to the employee's termination date. The transaction logs indicated that no updates were made by the former employee in the FLORIDA System. Absent the timely deactivation of former employee access privileges, the risk is increased that the access privileges could be misused by former employees or others.

Recommendation: The Department should ensure that the access privileges of former employees are deactivated in a timely manner pursuant to the *FLORIDA Security Guide*.

Finding No. 7: 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. 2011-141. 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. 8: Systems Development and Modification

Systems development and modification controls help guide implementation of new systems and ensure that only authorized modifications are made to existing systems. Effective program modification controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation.

Although the Department followed a standard systems development life cycle (SDLC) methodology, the methodology was not documented in writing and our audit disclosed that additional written guidance was needed. A similar finding was noted in prior audits of the Department, most recently our report No. 2011-141. An SDLC methodology details the procedures that are to be followed when systems and applications are being designed and developed, as well as when they are subsequently modified. Without a written SDLC methodology, there is an increased risk that management-intended controls to ensure authorized and appropriate systems development and modification will not be consistently followed.

Recommendation: The Department should establish a written SDLC methodology that details the procedures that are to be followed when systems and applications are designed, developed, and subsequently modified.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for two of the findings included in our report No. 2011-141 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 July 2011 through April 2012 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 the extent to which the Department has corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2011-141.

The scope of our audit focused on evaluating selected IT controls applicable to the FLORIDA System, including selected general IT controls over systems modification and logical and physical access security, and selected application IT controls and user controls relevant to the PA Component of the FLORIDA System.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the FLORIDA System, including the computing platform and related software, purpose and goals, and the basic data and business process flows though the PA Component.
- Obtained an understanding of key FLORIDA System PA Component application 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 calculation, and data exchange.
- Observed and evaluated the effectiveness of key FLORIDA System PA Component user account administration processes and procedures.
- Tested the effectiveness of controls over separation of duties of Department staff with access to the FLORIDA System PA Component. Specifically, we tested 109 user accounts to determine whether the access levels granted enforced an appropriate separation of duties between auxiliary and fiat creation and authorization.
- Evaluated on a sample basis the effectiveness of procedures for authorizing user access privileges to the PA Component and the appropriateness of the access privileges granted. Specifically, we sampled 60 user accounts to determine whether the access was authorized in writing and the profiles and security levels granted were appropriate.

- Evaluated on a sample basis the effectiveness of procedures for deactivating the PA Component access privileges of former employees. Specifically, we sampled 60 former employees who terminated employment with the Department between April 1, 2011, and November 22, 2011.
- 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.
- Tested the effectiveness of logical access controls over selected FLORIDA System IT resources. Specifically, we tested 122 user accounts within 18 groups with access to mainframe datasets to determine whether the access granted was appropriate.
- Tested the effectiveness of FLORIDA System password settings to evaluate the effectiveness of the settings in adequately protecting resources.
- Observed and evaluated key processes and procedures related to Department network and barrier controls.
- Observed and evaluated key Department program modification control processes and procedures for the FLORIDA System. Evaluated on a sample basis the effectiveness of controls over FLORIDA System modifications. Specifically, we sampled 11 of 49 modifications that were moved into production between July 1, 2011, and December 15, 2011, to determine whether the modifications were adequately approved, designed, tested, and implemented.
- Observed and evaluated key processes and procedures related to physical access controls protecting the FLORIDA System.
- Tested the effectiveness of physical access control procedures. Specifically, we tested 16 user accounts with access to the computer room at the Northwood Shared Resource Center to determine whether access granted was authorized and appropriate.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

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 July 31, 2012, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE



State of Florida
Department of Children and Families

Rick Scott
Governor

David E. Wilkins
Secretary

July 31, 2012

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

Dear Mr. Martin:

Thank you for your June 29th letter accompanying the preliminary findings and recommendations of your report on your Information Technology Audit of the Department of Children and Families Services, Florida Online Recipient Integrated Data Access (FLORIDA) System.

The Department generally concurs with the findings of your report. Enclosed is the Department's response to the specific recommendations you provided. If you have any questions, please contact Mr. Art Harwood at (850) 921-0676.

Sincerely,

David E. Wilkins
Secretary

Enclosure

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DCF RESPONSE TO 2012 PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Information Technology Operational Audit of the

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES SERVICES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM

FINDING # 1: USE OF SSNS

RECOMMENDATION: In the absence of establishing an imperative need for the use of the SSN, the Department should comply with State law by establishing another number to be used in the FLORIDA System rather than the SSN.

RESPONSE: The Department agrees with this finding and has been researching solutions to address it within the FLORIDA System. The following activities are being researched:

1. We are currently exploring the possibility of using the Florida Driver's License number or the State Issued ID card number as a unique identifier for the DCF employees.
2. Also, we are exploring adding a feature within the FLORIDA System to validate users through an identification verification process similar to the current customer process. It has been estimated that it would take approximately 2,000 hours to make this enhancement to the current FLORIDA ACCESS system.

However, DCF is actively pursuing procurement activities to replace the current system in the near future and the new system will accommodate correcting this finding.

FINDING # 2: SEPARATION OF DUTIES

RECOMMENDATION: The Department should take steps to minimize the likelihood that the FLORIDA System edit enforcing an appropriate separation of case management duties could be circumvented.

RESPONSE: The Department agrees with this finding. The FLORIDA System is designed to rely upon the Department Local and Headquarters' Security officer to correctly enter the information for each user to ensure the systematic controls that are in place are not circumvented. We are looking at edit enhancements to the current system to resolve this finding. This finding will also be eliminated with the installation of a new eligibility replacement system.

FINDING #3: DATA EXCHANGES

RECOMMENDATION: The Department should continue to seek solutions for ensuring that data exchange responses are processed within the required timeframe.

RESPONSE: The Department concurs with this finding. The ACCESS Program Office continues to stress the importance of processing data exchanges in a timely manner and ACCESS Quality Management continues to monitor this process. Critical to successful compliance is the ability to manage and display the appropriate data exchange workload. FLORIDA System has been unable to keep pace with updated policy and accompanying system development rendering more than half of the data exchanges received as duplicates or

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DCF RESPONSE TO 2012 PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Information Technology Operational Audit of the

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES SERVICES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM

redundant. Additionally, many exchanges post when no required action is needed; therefore, the potential impact on accuracy is artificially inflated, the percentage of overdue exchanges is misleading, and the added workload is managed through staff's effective prioritization. The FLORIDA System is extremely limited in its ability to process data exchanges without worker intervention, exasperated by the steep increase in program participation over the past few years. ACCESS Program Office conducted an in depth analysis of data exchange sources, current policy and system programming needs. ACCESS Technology has developed and proposed system program changes designed to display only meaningful information, and react to relevant data to eliminate human intervention, redundancy and waste as a possible resolution to this finding.

FINDING # 4: DOCUMENTATION OF USER ACCESS AUTHORIZATIONS

RECOMMENDATION: The Department should improve its FLORIDA System PA Component user account management procedures by ensuring that access authorization forms are appropriately completed, accurate, and maintained.

RESPONSE: The Department agrees with this finding. The Department relies upon our regional and headquarters security officers to follow existing access authorization request procedures as documented. In order to increase awareness and ensure compliance, DCF will continue to periodically audit and re-train the security officers on access authorization procedures. In addition, DCF will implement actions to improve the maintenance of user access documentation processes to ensure appropriate record retention.

FINDING # 5: APPROPRIATENESS OF ACCESS PRIVILEGES

RECOMMENDATION: The Department should remove the unnecessary and excessive access privileges and review the ongoing appropriateness of all access privileges granted to the FLORIDA System production datasets to ensure that access is commensurate with the requirements of employee job duties and to ensure the reliability of the above-described FLORIDA System IT resources.

RESPONSE: The Department agrees with this finding. DCF will perform a review of the NSRC mainframe technical support staff access and update any inappropriate privileges to insure that NSRC staff only has the access needed to do their assigned job.

FINDING # 6: TIMELY DEACTIVATION OF FORMER EMPLOYEE ACCESS PRIVILEGES

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DCF RESPONSE TO 2012 PRELIMINARY AND TENTATIVE AUDIT FINDINGS

Information Technology Operational Audit of the

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES SERVICES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM

RECOMMENDATION: The Department should ensure that the access privileges of former employees are deactivated in a timely manner pursuant to the FLORIDA Security Guide.

RESPONSE: The Department agrees with this finding. Corrective action has been completed.

- The Department worked with DCF's Human Resources group to establish a termination file that is sent to the regional and headquarters' security officer. This file is automatically generated from Peoples First and contains a listing of employees that separated from the Department. The DCF security officers have been instructed to use this file to terminate FLORIDA system access for individuals listed. This file is sent to the security officers on a daily basis.
- As a compensating control, the FLORIDA system automatically revokes the RACF account for the user after 45 days of inactivity. The FLORIDA system has been modified to send a monthly SMUM/RACF Reconciliation report to the security officers to ensure that any discrepancies between SMUM and RACF are resolved timely. RACF revokes user access after 45 days; the SMUM will continue to show that user as active, and these reports assist the security officer in verifying user access and will also assist inactivating users who no longer require system access.

FINDING # 7: SECURITY CONTROLS – PASSWORDS AND DATA TRANSMISSION

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 agrees with this finding and is working with the ACCESS team, the Department Security group, and NSRC Network staff to address this issue.

FINDING # 8: SYSTEMS DEVELOPMENT AND MODIFICATION

RECOMMENDATION: The Department should establish a written SDLC methodology that details the procedures that are to be followed when systems and applications are designed, developed, and subsequently modified.

RESPONSE: The Department has drafted a system development life cycle (SDLC) methodology document and is currently reviewing it. Once the review is complete, it will be determined whether the existing SDLC needs updating to address security or if it will be necessary to develop an enhanced version of the SDLC.