REPORT NO. 2010-066
JANUARY 2010

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

FLORIDA ONLINE RECIPIENT INTEGRATED DATA ACCESS (FLORIDA) SYSTEM

Information Technology Operational Audit

For the Period
July 1, 2008, Through June 30, 2009,
and Selected Actions from April 1, 2008

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF CHILDREN AND FAMILY SERVICES

Pursuant to Section 20.19(2)(a), Florida Statutes, the Secretary of the Department of Children and Family Services is appointed by the Governor, subject to confirmation by the Senate. George H. Sheldon served as Secretary during the audit period.

The audit team leader was Gwen Pacubas, 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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

Florida Online Recipient Integrated Data Access (FLORIDA) System

SUMMARY

The Florida Online Recipient Integrated Data Access (FLORIDA) System is a Statewide system operated and maintained by the Office of Information Technology Services within the Department of Children and Family Services (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 for the period July 1, 2008, through June 30, 2009, and selected actions from April 1, 2008. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2008-197.

The results of our audit are summarized below:

Application Controls

Finding No. 1: Contrary to Section 119.071(5)(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 issue was also disclosed in our report No. 2008-197.

Finding No. 2: As similarly noted in our report No. 2008-197, 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. This issue was also disclosed in our report No. 2008-197.

Security Controls

Finding No. 4: Documentation of authorization for the PA Component access privileges of some employees was missing, incomplete, or inaccurate. Similar issues were disclosed in our report No. 2008-197.

Finding No. 5: The Department did not timely revoke the PA Component access privileges of some former employees.

Finding No. 6: The PA Component and other IT resource access privileges of some employees and groups exceeded what was necessary for their job duties. Similar issues were noted in our report No. 2008-197.

Finding No. 7: The Department's written policies and procedures for the periodic review of FLORIDA System PA Component access privileges needed improvement. Additionally, a periodic review of FLORIDA System IT resource access privileges had not been performed.

Finding No. 8: The physical access authorization forms of some employees and contractors did not accurately document the computer room access privileges that were allowed.

Finding No. 9: Certain Department security controls related to passwords and network barrier and transmission controls needed improvement. Similar issues were disclosed in our report No. 2008-197.

Other General Controls

Finding No. 10: As similarly noted in our report No. 2008-197, the Department's systems development and modification policies and procedures needed improvement.

Finding No. 11: Program modification logs were not completed for some FLORIDA System program modifications, contrary to Department program change control procedures.

Finding No. 12: FLORIDA System hardware performance and capacity monitoring policies and procedures were not documented.

BACKGROUND

The Department of Children and Family Services (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 of Children and Family Services 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 Temporary Cash Assistance, Food Stamps, and Medicaid. 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 is functionally organized into two major components, Public Assistance (PA) and Child Support Enforcement (CSE). The 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 CSE Component is 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. Each component is maintained by separate groups within the Department's Office of Information Technology Services (OITS) Software Maintenance and Development Section.

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 an 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 audit report No. 2008-197, 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 SSNs were used. However, we have notified appropriate Department personnel of this issue.

Although the Department stated in writing the purpose for its collection of SSNs, 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 instead of another number. The use of the SSN was contrary to State law and increased the risk of improper disclosure of SSNs.

Recommendation: The Department should comply with State law by clearly establishing why the use of employee SSNs is imperative for the Department to perform its duties and responsibilities or alternatively establish another number to be used 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. An appropriate separation of duties precludes one person from controlling all stages of a process, a situation in which errors or irregularities could occur without timely detection.

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 instances where edits 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 issues in this report to avoid the possibility of compromising Department information. However, we have notified appropriate Department personnel of the specific issues. A similar finding was disclosed in our report No. 2008-197.

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 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 enhance the effectiveness of FLORIDA System controls to enforce an appropriate separation of case management duties.

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 there were numerous data exchange responses overdue. As of July 14, 2009, there were 645,753 (188,716 of which were responses that were verified upon receipt) overdue data exchange responses. In response to audit inquiry, Department staff 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 of ineligible individuals receiving benefits, as previously discussed in our report No. 2009-144, Finding No. FA-08-058 and our report No. 2008-197.

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 computer resources needed and prevent others from accessing the resources. Access controls include the use of access authorization forms to document the access privileges that have been authorized by management for system users.

According to the FLORIDA Security Guide, FLORIDA System user account administration (creating, changing, 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, change, or revoke a FLORIDA System user account. Required information on these forms includes first and last name, action required, user identification code (ID), security profile name, and security level. Other information is required depending on the nature of the request.

Our audit disclosed instances where, as discussed in the following paragraphs, the Department had not appropriately documented authorizations of user access privileges granted to some employees contrary to the FLORIDA Security Guide. 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.

For a sample of 22 FLORIDA System PA Component employee user accounts, we requested the corresponding access authorization forms to determine the level of access that had been authorized by management. For 6 of the 22 user accounts included in our sample, Department staff could not provide the authorization forms. A similar finding was disclosed in our report No. 2008-197. Department staff subsequently provided authorization forms for 2 of the 6 user accounts; however, the forms were dated after the audit period.

For the remaining 16 user accounts in our sample, we inspected the authorization forms that Department staff provided. For 6 of the 16 user accounts, the authorization forms were missing required information. Specifically:

- Six lacked the security profile.
- Three lacked the security level.
- One lacked the supervisor signature.

For 4 of the 16 user accounts, we determined that differences existed between the access privileges granted in the FLORIDA System versus those specified on the authorization forms. Specifically, 2 of the 4 user accounts had security profiles not matching what was specified on the forms, and 4 user accounts had security levels not matching

what was specified on the forms. These differences appeared to be the result of outdated information on the authorization forms. The security profiles and security levels associated with the 4 user accounts appeared appropriate based on the job duties of the employees to whom the 4 user accounts were assigned. In response to audit inquiry, Department staff provided an updated authorization form for one of the user accounts.

One of the 16 user accounts had an incorrect employee last name recorded both in the FLORIDA System and on the authorization form.

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

Finding No. 5: Revoking of Former Employee Access

Effective logical access controls include provisions for the timely revoking 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 revoked 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 a written request for the employee's access privileges to be revoked.

Our audit disclosed that the Department did not timely revoke 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 35 former employees who terminated employment between July 2008 and May 2009, we reviewed FLORIDA System PA Component user access listings to determine whether the former employees' access privileges were revoked in a timely manner. For 24 of the 35 former employees included in our sample, access privileges had not been timely revoked in the FLORIDA System. The 24 former employees retained access privileges from 7 to 343 days after their termination dates. Of the 24 former employees:

- Access privileges for 21 of the former employees were retained in the FLORIDA System as of the date that the user access listing was provided to us for review.
- Documented requests for access privileges to be revoked were not available for 18 of the former employees.
- Although documented requests for access privileges to be revoked were available for 3 former employees, their user IDs had been omitted from the request.
- Although documented requests for access privileges to be revoked were available for 3 former employees, their access was not revoked for 7 to 72 days after their termination dates.

We noted one user ID belonging to a former employee included in our sample that was used after her termination date. All other user IDs in the sample either had never been used or had not been used after the termination date. Through other audit procedures, we identified two user IDs belonging to a former employee that did not have access privileges revoked in the FLORIDA System for 860 days after his termination date. The access privileges associated with the two user IDs were also used after his termination date. In response to audit inquiry, Department staff stated that these user IDs belonged to former employees who accepted other State positions outside of the Department. These former employees continued to use their user IDs because their new State positions involved responsibilities that required access to the FLORIDA System. However, Department staff acknowledged that the former employees

had access privileges beyond what was necessary for their new State positions outside of the Department and stated that the access privileges have been appropriately updated.

Recommendation: The Department should ensure that the access privileges of former employees are revoked in a timely manner. As provided in the FLORIDA Security Guide, the Department should prepare written requests for the revoking of former employee access and retain the requests for use in the periodic review of the appropriateness of employee access privileges as further discussed in Finding No. 7.

Finding No. 6: Appropriateness of Access Privileges

Limiting system user 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 system data.

Our audit disclosed that 4 of 30 employees included in our sample with FLORIDA System PA Component access privileges had user IDs with security profiles providing access privileges that were not necessary for their job positions. In response to audit inquiry, Department staff indicated that the security profile for one of the user IDs was subsequently changed to a more appropriate profile.

Our audit also disclosed that some groups and individual employees had unnecessary and excessive access privileges to datasets containing FLORIDA System operating system logs, database logs, and production programs and job control language (JCL). Similar issues were noted in our report No. 2008-197. Specifically:

- The Database and the Quality and Implementation and Control (QIC) groups had the ability to change operating system logs that recorded activities performed on datasets. Although these groups needed access to other datasets stored under the high-level identifier that contained the operating system logs, they did not need access to all datasets. Under these conditions, the risk is increased that unauthorized modifications may be made to the logs, rendering the logs unreliable for use in detecting inappropriate dataset access. In response to audit inquiry, Department staff indicated that QIC staff access was updated to only allow access to specific datasets needed.
- The QIC group had the ability to change database logs that recorded all transactions performed in the database. Staff in this group did not need this access to perform their job duties. These conditions increased the risk that unauthorized modifications may be made to the logs, rendering the logs unreliable for use in detecting inappropriate transactions.
- One employee, a user within the Data Security group, had ALTER access to libraries that contained FLORIDA System production programs and JCL. This user did not need this access to perform his job duties. This increased the risk of unauthorized modification or destruction of production programs and JCL. In response to audit inquiry, Department staff indicated that the employee's access was subsequently removed.

Recommendation: The Department should limit access privileges to the FLORIDA System PA Component and other supporting IT resources to only what is needed in the performance of assigned job duties.

Finding No. 7: Periodic Review of Access

Periodic reviews of user access privileges help ensure that user access privileges remain appropriate. Written policies and procedures help provide guidance and direction to employees responsible for performing such reviews by allowing for better communication and consistent application of management-intended controls.

According to Department security staff, Department system owners are responsible for ensuring that the access granted to users is appropriate for their system. However, no Departmentwide policy or procedure existed to require system owners to perform periodic reviews of access privileges.

According to the FLORIDA Security Guide, regional security officers are responsible for performing periodic reviews of the FLORIDA System to determine which user IDs are not being used. However, no written procedures existed that detailed how the review was to be performed, specifically how often the reviews were to be performed and actions that regional security officers should take when discrepancies in access privileges were found.

In response to audit inquiry, Department staff indicated that the last review of FLORIDA System user access privileges was performed in February and March 2009 at the direction of the ESS Program Office and Headquarters security officer. However, a review of access privileges to FLORIDA System IT resources, including operating system logs, database logs, and production programs and JCL, had not been performed.

As demonstrated by the excessive or unnecessary IT resource access privileges disclosed in Finding No. 6, the lack of periodic reviews of access privileges increases the risk that excessive or inappropriate access privileges will not be timely detected or revoked. Under such conditions, the risk is increased of unauthorized disclosure, modification, and destruction of FLORIDA System data and IT resources.

Recommendation: The Department should establish written policies and procedures that provide guidance to system owners for performing periodic reviews of access privileges, including FLORIDA System specific procedures. The Department should also ensure that such reviews are performed periodically and in a manner pursuant to management's expectations.

Finding No. 8: Physical Access Controls

Effective security controls include physical access controls to ensure that access to premises, buildings, and areas is appropriate. Physical access controls include documenting and maintaining access authorizations and changes thereto on standard forms and periodically reviewing and comparing access privileges documented on the forms to access privileges granted to ensure that access is appropriate.

According to the Department's Physical Security Guide, individuals (employees and contractors) must submit an approved badge authorization form to be issued a badge to enter the Technology Center. The form must be signed by the individual's supervisor and the appropriate access and hours of access must be specified on the form. Badge access to the computer room is provided only if individuals need access to perform their job functions.

Our audit disclosed that access to the computer room for two individuals did not match what was documented on their badge authorization forms. Although Department staff stated that their access privileges were appropriate based on their job functions, their authorization forms had not been updated to reflect the access granted. In response to audit inquiry, Department staff indicated that they subsequently updated the badge authorization forms to document the access that was currently authorized for these two individuals.

The Department converted to a new badge system in July 2008, during which time badge accounts were manually reviewed and entered from the previous system. Another review of physical access was not performed subsequent to the conversion to the new badge system. However, in response to audit inquiry, the Department established written procedures on July 30, 2009, that provided for an annual review of physical access.

Without accurate authorization forms documenting individuals' approved physical access privileges, an effective periodic review of access cannot be performed. This increases the risk that individuals will have excessive or

inappropriate physical access privileges. Excessive or inappropriate physical access privileges increase the risk of unauthorized entry and the misuse, loss, or destruction of IT assets.

Recommendation: The Department should ensure that changes in individuals' physical access privileges are documented and authorized on badge authorization forms. The Department should continue to perform periodic reviews of physical access privileges.

Finding No. 9: Security Controls – Passwords and Network

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. As similarly noted in our report No. 2008-197, our audit disclosed certain Department security controls related to passwords and network barrier and transmission controls 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. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

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

Other General Controls

Finding No. 10: Systems Development and Modification

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

Although the Department had established some written program change control procedures, our audit disclosed that additional written guidance was needed and some existing procedures were outdated. Similar issues were disclosed in our report No. 2008-197. Specifically:

- Although the Department followed a standard systems development life cycle (SDLC) methodology, the methodology was not documented in writing. 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.
- Procedures were not documented for the appropriate use of an internal ID code for Endevor, the software used to control and monitor the development and implementation of mainframe programs. QIC staff who were responsible for moving mainframe programs into the production environment had access to the internal ID code that could be used to perform various tasks, such as running batch jobs and archiving programs. Use of the internal ID code by QIC staff is only necessary when archiving programs. In response to audit inquiry, Department staff stated that a programming change was implemented in July 2008 that prevented programs from being moved into the production environment using the Endevor internal ID code. During testing of FLORIDA System program modification controls, we noted parameters (a type of program within Endevor) that were moved into the production environment using the Endevor ID code. In response to audit inquiry, Department staff indicated that the internal Endevor ID code was limited to QIC staff and it was appropriate for QIC staff to use the ID code. Department staff further stated that the programming change in July 2008 did

not prevent parameters from being moved into the production environment using the Endevor internal ID code. In these circumstances, any activity performed in Endevor using the internal ID code could not be definitively traced to the responsible individual in QIC, which increases the risk of the Department not being able to establish responsibility for inappropriate activities within Endevor, should they occur.

- FLORIDA System program change control procedures were out of date. Specifically, the FLORIDA Standard Practice Document T-213 and the ServiceCenter FLORIDA Change Management User Guide were last updated on November 1, 2002, and February 13, 2003, respectively, and referenced obsolete program change documentation. Without current program change control procedures, there is an increased risk of unauthorized or erroneous changes being made to programs. In response to audit inquiry, Department staff provided an updated FLORIDA Standard Practice Document T-213, dated July 13, 2009.

Recommendation: The Department should establish a written SDLC methodology and ensure that all systems development and modification policies and procedures are up to date and reflect appropriate control activities.

Finding No. 11: Program Modification Logs

According to the Department's Standard Operating Procedures (SOP C-31) Computer Operations Job Control Language, programmers who make changes to programs are required to document the date of the change, description of the change, and name of the person making the change in program modification logs. Our audit disclosed 7 of 30 FLORIDA System program modifications included in our sample of modifications implemented from July 2008 through May 2009 that did not have documentation of changes made to programs in the program modification logs. Although the related ServiceCenter tracking numbers were found in the comments section of the programs, the program modification log was not completed with the details of the modification. Without appropriate program modification logging, program changes cannot readily be traced back to supporting documentation of authorization and approvals, limiting the Department's ability to monitor the program change process.

Recommendation: The Department should ensure that its programming change control policies are followed and that program changes are appropriately documented in the program modification logs.

Finding No. 12: FLORIDA System Hardware Performance and Capacity Monitoring

System performance and capacity monitoring helps ensure that IT resources supporting business requirements are continually available. Monitoring activities include collecting and evaluating data for the purposes of maintaining and tuning current performance within IT; addressing such issues as contingency requirements, current and projected workloads, storage plans, and resource acquisition; and reporting delivered service availability.

The Mainframe Technical Support (MTS) group within the OITS Production Services group was responsible for FLORIDA System hardware performance and capacity management. MTS performed daily monitoring of the FLORIDA System for response time and capacity-related issues and produced a monthly summary report of system performance. Our audit disclosed, however, that FLORIDA System hardware performance and capacity monitoring policies and procedures were not documented in writing. Without written FLORIDA System hardware performance and capacity monitoring policies and procedures, the risk is increased that appropriate hardware performance and capacity monitoring will not be performed consistently in a manner pursuant to management's intent.

Recommendation: The Department should ensure that written policies and procedures for hardware performance and capacity monitoring are established, communicated, and periodically reviewed to ensure that FLORIDA System hardware is effectively managed and controlled.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2008-197.

SCOPE, OBJECTIVES, 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 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, and reliability of data; and the safeguarding of IT resources.
- Determine the extent to which the Department corrected, or were in the process of correcting, deficiencies disclosed in our report No. 2008-197.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

The scope of our audit focused on evaluating selected IT controls applicable to the FLORIDA System during the period July 1, 2008, through June 30, 2009, and selected actions from April 1, 2008.

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 processing flows though the PA component.
- Obtained an understanding of the FLORIDA System PA component application controls, including input, processing, output, and user controls.
- Obtained an understanding of general IT controls related to the FLORIDA System.
- Observed, documented, tested, and evaluated key processes and procedures related to the appropriateness of selected application controls, including separation of duties, exception reporting, and transaction logging within the PA component.
- Observed, documented, tested, and evaluated key processes and procedures related to the appropriateness of FLORIDA System PA component user account administration procedures.

- Observed, documented, and evaluated key processes and procedures related to FLORIDA System hardware performance and capacity monitoring.
- Observed, documented, and evaluated key processes and procedures related to the Department security plan and program, including risk assessments, security policies and procedures, and security awareness training.
- Observed, documented, and evaluated key processes and procedures related to physical controls protecting the FLORIDA System.
- Observed, documented, tested, and evaluated key processes and procedures related to logical access controls over FLORIDA System IT resources, including adequacy of review and removal of access privileges, adequacy of review of access to FLORIDA System computer resources, and the adequacy of password controls related to the FLORIDA System.
- Observed, documented, tested, and evaluated key processes and procedures related to the Department program change control processes for making modifications to the FLORIDA System.
- Observed, documented, tested, and evaluated key processes and procedures related to Department network and barrier controls.
- 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 December 9, 2009, 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

Charlie Crist
Governor

George H. Sheldon
Secretary

December 9, 2009

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

Dear Mr. Martin:

Thank you for your November 9 letter accompanying the preliminary findings and recommendations of the *Information Technology Audit of the Department of Children and Families Services, Florida Online Recipient Integrated Data Access (FLORIDA) System, for the period July 1, 2008 through June 30, 2009 with selected Department actions from April 1, 2008.*

Enclosed is the Department's response to your audit recommendations. As you may remember, the Northwood Shared Resource Center (NSRC) became a separate agency on July 1, 2009. However, because the Northwood data center was part of the Department of Children and Families (DCF) during the audit period, DCF responded to these findings with guidance from NSRC staff. In the future, DCF will be happy to assist NSRC in responding to any recommendations directed to them on these subjects.

If I may be of further assistance, please let me know.

Sincerely,

George H. Sheldon
Secretary

Enclosure

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DCF Response to Follow-up of the OAG 2008-197 Preliminary and Tentative Audit Findings and Recommendations to the FLORIDA System Audit for the Period July1, 2008 through June 30, 2009.

Finding #1	Use of SSNs – Contrary to Section 119.071(5)(a), FS, the Department used certain employee 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 issue was also disclosed in our report #2008-197.
	Recommendation: The Department should comply with State law by clearly establishing why the use of employee SSNs is imperative for the Department to perform its duties and responsibilities or alternatively establish another number to be used rather than the SSN.
DCF Response	We agree with the recommendation and will change the form to include the imperative need. Although we would prefer to use an identifier other than the SSN, there is currently no identifier other than SSN that is reliably unique, and this change would also require funds to identify and associate existing client data with a new number.
Finding #2	Separation of Duties – As similarly noted in our report #2008-197, FLORIDA System edits designed to prevent employees from performing incompatible case management functions could be circumvented in certain instances.
	Recommendation: The Department should enhance the effectiveness of FLORIDA System controls to enforce an appropriate separation of case management duties.
DCF Response	We agree with this recommendation and will make enhancements to support it.
Finding #3	Data Exchanges – The Department had numerous unprocessed overdue data exchange responses. This issue was also disclosed in our report #2008-197.
	Recommendation: The Department should continue to seek solutions for ensuring that data exchange responses are processed within the required time frames.
DCF Response	We agree. The ACCESS Program Office continues to stress the importance of processing data exchanges in a timely manner. Also, the ACCESS Quality Management Bureau continues to monitor this process. Additionally, the ACCESS Technology and Systems Design Bureau continues to work with Information Systems staff to automatically process as many of these reviews as possible. Currently, data exchanges are posted as we receive them. We would like to note, however, that the SNAP program does not require staff to process data exchange until review. Therefore, data exchanges that may appear to be overdue using general data exchange timelines (rather than specific SNAP guidelines) are in fact not overdue. We plan to make programming changes to post SNAP data exchanges only at review to make this difference clearer, but have not yet been able to prioritize this work due to limited programming staff.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding #4	Documentation of User Access Authorizations – Documentation of authorization for the PA Component access privileges of some employees was missing, incomplete, or inaccurate. Similar issues were disclosed in our report #2008-197.
	Recommendation: The Department should improve FLORIDA System PA Component user account management procedures by ensuring that access authorization forms are appropriately completed and maintained.
DCF Response	We agree with this recommendation and will develop a refresher course on FLORIDA security controls.
Finding #5	Revoking of Former Employee Access – The Department did not timely revoke the PA Component access privileges of some former employees.
	Recommendation: The Department should ensure that the access privileges of former employees are revoked in a timely manner. As provided in the FLORIDA Security Guide, the Department should prepare written requests for the revoking of former employee access and retain the requests for use in the periodic review of the appropriateness of employee access privileges as further discussed in Finding #7.
DCF Response	We agree with this recommendation and we will continue to remind supervisors to notify their local security officer when employees leave the Department. This will also be included as a component of the refresher training that is provided to Security Officers.
Finding #6	Appropriateness of Access Privileges – The PA Component and other IT resource access privileges of some employees and groups exceeded what was necessary for their jobs duties. Similar issues were noted in our report #2008-197.
	Recommendation: The Department should limit access privileges to the FLORIDA System PA Component and other supporting IT resources to only what is needed in the performance of assigned job duties.
DCF Response	We agree with this recommendation and will develop a refresher course on FLORIDA security controls.
Finding #7	Periodic Review Access – The Department's written policies and procedures for the periodic review of FLORIDA System PA Component access privileges needed improvement. Additionally, a periodic review of FLORIDA System IT resource access privileges had not been performed.
	Recommendation: The Department should establish written policies and procedures that provide guidance to system owners for performing periodic reviews of access privileges, including FLORIDA System specific procedures. The Department should also ensure that such reviews are performed periodically and in a manner pursuant to management's expectations.
DCF Response	We agree with this recommendation and have started sending out security access list to all security officers for their review. These lists will go out every other month. The next list will go out in December.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding #8	Physical Access Controls – The physical access authorization forms of some employees and contractors did not accurately document the computer room access privileges that were allowed.
	Recommendation: The Department should ensure that changes in individuals' physical access privileges are documented and authorized on badge authorization forms. The Department should continue to perform periodic reviews of physical access privileges.
DCF Response	We agree with this finding. We are implementing processes that will help ensure that the badge authorization forms are updated when access changes are made. Also, we are going to schedule a review of physical access privileges within the next 60 days.
Finding #9	Security Controls – Passwords and Network – Certain Department security controls related to passwords and network barrier and transmission controls needed improvement. Similar issues were disclosed in our report #2008-197.
	Recommendation: The Department should improve password and network barrier and transmission controls to ensure the confidentiality, integrity, and availability of data and IT resources.
DCF Response	We agree with this recommendation and will improve password and network controls.
Finding #10	Systems Development and Modification – As similarly noted in our report #2008-197, the Department's systems development and modification policies and procedures needed improvement.
	Recommendation: The Department should establish a written SDLC methodology and ensure that all systems development and modification policies and procedures are up to date and reflect appropriate control activities.
DCF Response	We agree with this recommendation and are in the process of updating the System Development and Modification Procedures.
Finding #11	Program Modification Logs – Program modification logs were not completed for some FLORIDA System program modifications, contrary to Department program change control procedures.
	Recommendation: The Department should ensure that its programming change control policies are followed and that program changes are appropriately documented in the program modification logs.
DCF Response	We agree with this recommendation and have made changes to the Endeavor process to ensure that all program modification logs are documented prior to the change moving to production.
Finding #12	FLORIDA System Hardware Performance and Capacity Monitoring – FLORIDA System hardware performance and capacity monitoring policies and procedures were not documented.
	Recommendation: The Department should ensure that written policies and procedures for hardware performance and capacity monitoring are established, communicated, and periodically reviewed to ensure that FLORIDA System hardware is effectively managed and controlled.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

DCF/NSRC Response	The Northwood Shared Resource Center (NSRC) will work to document the capacity planning and reporting policy and procedures. Effective July 1, 2009, the Department of Children and Families (DCF) Northwood data center became one of the three statewide shared resource centers known as the Northwood Shared Resource Center (NSRC). With the exception of application development, all data center hardware, software, staff, contracted services, and facility resources performing data center management & operations, security, production control, backup & recovery, disaster recovery, system administration, database administration, system programming, job control, production control, print, storage, technical support, help desk, & managed services were transferred to the NSRC.