REPORT NO. 2011-141
MARCH 2011

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

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 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 Angie Beam 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 FAMILY SERVICES

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 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. We also determined the status of corrective actions regarding audit findings disclosed in our report No. 2010-066.

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 finding was also noted in prior audits of the Department, most recently our report No. 2010-066.

Finding No. 2: The Department had numerous unprocessed overdue data exchange responses. Similar findings were noted in prior audits of the Department, most recently our report No. 2010-066.

SECURITY CONTROLS

Finding No. 3: As similarly noted in prior audits of the Department, most recently our report No. 2010-066, documentation of authorization for the FLORIDA System PA Component access privileges of some employees was missing, incomplete, or inaccurate.

Finding No. 4: As similarly noted in prior audits of the Department, most recently our report No. 2010-066, the Department did not timely disable the PA Component access privileges of some former employees.

Finding No. 5: The IT resource access privileges of a database group exceeded what was necessary for their job duties. A similar finding was also noted in prior audits of the Department, most recently our report No. 2010-066.

Finding No. 6: As similarly noted in our report No. 2010-066, the physical access authorization forms of some employees and contractors did not accurately document the computer room access privileges that were allowed. Also, the Department's informal processes for the modification and removal of physical access privileges were not documented in the form of written procedures.

Finding No. 7: Certain Department security controls related to passwords needed improvement. Similar findings were noted in prior audits of the Department, most recently our report No. 2010-066.

OTHER GENERAL CONTROLS

Finding No. 8: As similarly noted in prior audits of the Department, most recently our report No. 2010-066, the Department's systems development and modification policies and procedures needed improvement.

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 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 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. The FLORIDA System is housed and operated at the Northwood Shared Resource Center.

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. 2010-066, 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.

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: 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 as the unique identifier rather than the SSN.

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 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 August 23, 2010, there were 602,580 (approximately 280,496 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 similarly noted in prior audits of the Department, most recently our report No. 2010-165, Finding FA 09-059 and report No. 2010-066.

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. 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 employees contrary to the FLORIDA Security Guide. A similar finding was noted in prior audits of the Department, most recently our report No. 2010-066. 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.

We requested access authorization forms for a sample of 32 active FLORIDA System PA Component users as of August 9, 2010. For one of the 32 users included in our sample, Department staff could not provide the authorization form. Of the 31 authorization forms on file, 5 forms lacked required information. Specifically:

- Three forms lacked both the security profile and level.
- Two additional forms lacked the security profile.

Additionally, access levels shown as authorized on 2 additional forms did not match the access levels actually granted in the FLORIDA System. The access levels granted, however, did not appear excessive for the job duties of the FLORIDA user listed on the form.

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. 4: Timely Disabling of Former Employee Access Privileges

Effective access controls include provisions for the timely disabling 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 disabled 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 disabled.

As similarly noted in prior audits of the Department, most recently our report No. 2010-066, our audit disclosed that the Department did not timely disable 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 20 former employees who terminated employment between July 1, 2009, and August 9, 2010, we reviewed FLORIDA System PA Component user access listings to determine whether the former employees' access privileges were disabled in a timely manner. For 15 of the 20 former employees included in our sample, access privileges had not been timely disabled in the FLORIDA System. The 15 former employees retained access privileges from 2 to 273 days after their termination dates. Of the 15 former employees:

- Access privileges for 10 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. Department staff subsequently disabled FLORIDA System access privileges for these former employees.
- Documented requests for access privileges to be disabled were not available for 8 former employees.

None of the user identifications (IDs) and associated access privileges belonging to the 15 former employees had been used after the termination dates. Nevertheless, absent the timely disabling of former employee access privileges, the risk was 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 disabled in a timely manner pursuant to the FLORIDA Security Guide.

Finding No. 5: 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 the Database group had the ability to modify operating system logs that recorded activities performed on datasets. This access was unnecessary for the performance of the duties of the Database group. Under these conditions, the risk was increased that unauthorized modifications could be made to the logs, rendering the logs unreliable for use in detecting inappropriate dataset access. In response to audit inquiry, Department staff subsequently removed the Database group's ability to modify the operating system logs. A similar issue was noted in prior audits of the Department, most recently our report No. 2010-066.

Recommendation: The Department should review the ongoing appropriateness of access privileges to the operating system logs to ensure the reliability of the logs as a tool for monitoring operating system activity.

Finding No. 6: 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 modifications 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. Also, physical access activities need complete, well-documented policies and procedures to describe management's expectations for the activities.

According to the Department's Physical Security Guide, individuals (employees and contractors) with an approved badge authorization form will 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 six individuals did not match what was documented on their badge authorization forms. Four of the six individuals had been granted more access than was authorized on the form. 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. A similar finding was noted in our audit report No. 2010-066.

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.

Our audit further disclosed that, although the Department had informal processes in place for handling modification and removal of physical access privileges, the processes were not documented in the form of written procedures. Absent written procedures, the risk is increased that physical access controls may not be followed consistently and in a manner pursuant to management's expectations.

Recommendation: The Department should ensure that modifications in individuals' physical access privileges are documented and authorized on badge authorization forms. The Department should also establish written procedures to document management's expectations for the modification and removal of physical access privileges.

Finding No. 7: Security Controls – Passwords

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 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. A similar finding was noted in prior audits of the Department, most recently our report No. 2010-066. Without adequate security controls related to passwords, 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 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 had established some written program modification control procedures, our audit disclosed that additional written guidance was needed and some existing procedures were outdated. Similar issues were noted in prior audits of the Department, most recently our report No. 2010-066. 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 indicated that the internal Endevor ID code was limited to QIC staff. However, Department staff subsequently reduced the number of users with access from ten to four. 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 modification control procedures were inaccurate. Specifically, the FLORIDA Standard Practice Document T-213 and the draft Service Center FLORIDA Change Management User Guide were last updated on August 26, 2009, and November 23, 2010, respectively, and contained contradictory information. Without accurate program modification control procedures, there is an increased risk of unauthorized or erroneous modifications being made to programs.

Recommendation: The Department should establish a written SDLC methodology and ensure that all systems development and modification procedures accurately reflect the control activities established by management.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for some findings included in our report No. 2010-066 that were applicable to the scope of this audit. Corrective actions were not taken for many of the prior audit findings as described in the findings above. Portions of Finding No. 9 and all of Finding No. 12 of report No. 2010-066 were followed up on in our IT operational audit of the Northwood Shared Resource Center, report No. 2011-082.

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 2010 through November 2010 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 corrected, or were in the process of correcting, deficiencies disclosed in our report No. 2010-066.

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, documented, and evaluated the effectiveness of key application control processes and procedures, including eligibility determination and cutoff, benefit calculation, and data exchange.

- Observed, documented, 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 91 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 32 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 disabling the PA Component access privileges of former employees. Specifically, we sampled 20 user accounts of former employees who terminated employment with the Department between July 1, 2009, and August 9, 2010.
- Obtained an understanding of general IT controls related to the FLORIDA System.
- Observed, documented, 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 146 user accounts within 21 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, documented, and evaluated key processes and procedures related to Department network and barrier controls.
- Observed, documented, 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 29 modifications that were moved into production between July 1, 2009, and July 25, 2010, to determine whether the modifications were adequately approved, designed, tested, and implemented.
- Observed, documented, and evaluated key processes and procedures related to physical access controls protecting the FLORIDA System.
- Evaluated on a sample basis the effectiveness of physical access control procedures. Specifically, we sampled 30 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 February 28, 2011, the 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

David E. Wilkins
Secretary

February 28, 2011

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

Dear Mr. Martin:

Thank you for your February 1 letter accompanying the preliminary findings and recommendations of your report on your Information Technology Operational Audit of the Department of Children and Family 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 Ms. Lori Schultz, with our Information Systems Office, at (850) 487-8902.

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

Sincerely,

David E. Wilkins
Secretary

Attachment

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

RESPONSE TO 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 No. 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 as the unique identifier rather than the SSN.

Department Response: The Department concurs with this finding and continues to look for other viable options.

We have looked at other ways to identify employees uniquely, including the People First ID. However, whenever an employee leaves employment and returns later, a new People First ID is assigned, and therefore an individual is not uniquely identified. In addition, many of our users are contractors, for whom People First IDs are not available. We explored the use of pseudo People First IDs, but People First does not assign them. If the department created the pseudo IDs externally, there is no crosswalk or control that would prevent the same numbers being assigned to employees as actual People First IDs. Therefore, we have mitigated the use of social security numbers as required by section 119.071 (5) (a), F.S., and included language reviewed and approved by the Office of General Counsel in our security forms

We have reviewed the cost to create a clearance process for workers in which the system would create a unique identifying number for each employee; currently we do not have the funding to make the changes necessary to implement this process.

Finding No. 2: Data Exchanges

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

Department Response: The Department concurs with this finding. The ACCESS Program Office continues to stress the importance of processing data exchanges in a timely manner. Also, ACCESS Quality Management continues to monitor this process. Additionally, ACCESS Technology continues to work with Information Technology Services staff to automatically process as many of these reviews as possible. Several exchanges that are considered verified upon receipt have been automated since the last audit, such as the receipt of Florida Retirement Income (DEFR) and the initial receipt of Social Security and Supplemental Security Income (DESD and DEBB). Currently, data exchanges are posted as we receive them. We 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

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

RESPONSE TO 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

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.

Finding No. 3: 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.

Department Response: The Department concurs with this finding. The Department relies upon our regional and headquarters security officers to implement the access requests as documented. We will continue to periodically audit and train the security officers to only complete authorizations if they are properly documented.

Finding No. 4: Timely Disabling of Former Employee Access Privileges

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

Department Response: The Department concurs with this finding. The Department depends on supervisors submitting the revocation request to their regional security officer for timely removal of employees. As a compensating control, the FLORIDA system automatically revokes the RACF account for the user after 45 days of inactivity.

Currently, we send a monthly SMUM/RACF Reconciliation report to the security officer to ensure that any discrepancies between SMUM and RACF are resolved timely. RACF revokes 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.

We are currently in discussion with Human Resources to determine if an automated report of employee terminations can be generated and sent to the security officers (weekly, biweekly or monthly) to facilitate timely removal of system access. This report will ensure that any terminations that were not submitted for revocation by the supervisor would be captured.

Finding No. 5: Appropriateness of Access Privileges

Recommendation: The Department should review the ongoing appropriateness of access privileges to the operating system logs to ensure the reliability of the logs as a tool for monitoring operating system activity.

EXHIBIT A
MANAGEMENT'S RESPONSE (CONTINUED)

RESPONSE TO 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

Department Response: The Department concurs with this finding. The Department has removed the database group's access to modify the system logs. We will continue to audit this item periodically to ensure compliance.

Finding No. 6: Physical Access Controls

Recommendation: The Department should ensure that modifications in individuals' physical access privileges are documented and authorized on badge authorization forms. The Department should also establish written procedures to document management's expectations for the modification and removal of physical access privileges.

Department Response: The Department concurs with this finding. We will continue to monitor this through periodic badge and access form reviews. We will also work to strengthen our written procedures for granting and modifying physical access.

Finding No. 7: Security Controls – Passwords

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

Department Response: The Department concurs with this finding.

Finding No. 8: Systems Development and Modification

Recommendation: The Department should establish a written SDLC methodology and ensure that all systems development and modification procedures accurately reflect the control activities established by management.

Department Response: The Department is currently reviewing its system development life cycle (SDLC) methodology and considering either updating the current SDLC to address security or developing a new SDLC.

Changes have been made to the Endevor internal processes to ensure that the Endevor internal ID code (NDVR ID) cannot be used for executing production packages or running batch jobs. This ID can only be used for archiving programs. The execution of production packages and the running of batch jobs are performed by individual QIC staff using their unique user IDs, so that any activity performed can be traced back to the responsible individual in QIC.

FLORIDA Standard Practice Document T-213 is currently being reviewed and updated. The Service Center FLORIDA Change Management User Guide has been reviewed and updated and will be posted to the intranet site. Both documents will be reviewed for consistency before publication.