



# AUDITOR GENERAL

DAVID W. MARTIN, CPA



## DEPARTMENT OF CHILDREN AND FAMILY SERVICES FLORIDA ON-LINE RECIPIENT INTEGRATED DATA ACCESS SYSTEM Information Technology Audit

### SUMMARY

The Florida On-line Recipient Integrated Data Access (FLORIDA) System is a Statewide system operated and maintained by the Economic Self-Sufficiency Services (ESS) Program Office and Office of Information Systems within the Department of Children and Family Services (Department) to assist in public assistance program eligibility determination and benefit issuance. Our audit of the FLORIDA System focused on evaluating selected information technology (IT) controls applicable to the Public Assistance component of the FLORIDA System for the period October 2007 through March 2008, with selected actions taken from July 1, 2006, and determining the status of corrective actions regarding prior audit findings disclosed in audit report No. 2005-106. We also evaluated selected systems modification and application controls over the Automated Community Connection to Economic Self-Sufficiency Web Application and the Integrated Benefit Recovery System for the period.

The results of our audit are summarized below:

**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. Specific details of how the SSN was used are not disclosed in this report to avoid the possibility of compromising Department information. However, appropriate Department personnel have been notified of this issue.

**Finding No. 2:** In certain instances, a separation of duties within the FLORIDA System was either not in place or was ineffective. Specific details of this control deficiency are not disclosed in this report to avoid the possibility of compromising Department information. However, appropriate Department personnel have been notified of the specific instances noted.

**Finding No. 3:** The Department lacked FLORIDA System exception reports and related procedures to detect potential employee fraud. Additionally, the Department had numerous unprocessed overdue data exchange responses.

**Finding No. 4:** The Department did not maintain an adequate log of user activity within the FLORIDA System.

**Finding No. 5:** Certain Department security controls protecting the FLORIDA System and related IT resources were deficient.

**Finding No. 6:** The organizational placement of the Information Security Manager (ISM) and the security function within the Department did not maximize the effectiveness of the security function or reflect an appropriate level of importance and priority of security within the Department.

**Finding No. 7:** The Department's IT risk management procedures needed improvement.

**Finding No. 8:** The Department's systems development and modification controls 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, the Department is designated in Section 409.031, Florida Statutes, 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 Rules 65A-1.203, Florida Administrative Code, the Economic Self-Sufficiency Services (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 System to assist in eligibility determination and benefit issuance for public assistance programs.

The FLORIDA System is functionally organized into three major components: Public Assistance, Child Support Enforcement, and Client Registration. The Public Assistance component is composed of numerous application modules that function to collect and evaluate client information, such as income and asset information, to determine eligibility of a family or individual and calculate and generate public assistance benefits. The Child Support Enforcement 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. The Client Registration component is used for entering demographic information of people who need financial, medical, and child support assistance into the FLORIDA System.

**FINDINGS AND RECOMMENDATIONS**

**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), Florida Statutes, an agency shall 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.

The Department collected and used certain employee SSNs in the FLORIDA System. Specific details of how the SSN was used are not disclosed in this report to avoid the possibility of compromising Department information. However, appropriate Department personnel have been notified of this matter.

Although the Department stated in writing the purpose for its collection of certain employee SSNs, no specific authorization existed in law for the Department to collect the SSNs of FLORIDA System users and the Department had not established the imperative need to use the SSN, rather than 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.

To maintain an appropriate separation of duties in the public assistance area, the Department's practice was to prohibit any one caseworker from performing all aspects of managing a recipient's case, such as registering a client, entering eligibility data, and authorizing benefits. For example, if a caseworker was responsible for registering a client, the caseworker was prohibited from entering client eligibility data and authorizing benefits.

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 system users from registering a client and authorizing benefits for the client could be circumvented.

Additionally, in certain circumstances, caseworkers had the capability to both authorize and perform overrides of eligibility determinations and benefit calculations performed by the FLORIDA System. Department practice was for the authorization of the overrides to be performed by the caseworker's supervisor. In response to audit inquiry, Department staff stated that a programming change request was made to implement an edit to restrict the ability to authorize and perform overrides in the specific circumstances noted.

Specific details of this control deficiency are not disclosed in this report to avoid the possibility of compromising Department information. However, appropriate Department personnel have been notified of the specific instances noted.

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 ensure that additional controls are implemented to enforce an appropriate separation of duties with regard to client registration, eligibility determination, and benefit authorization in the FLORIDA System.

---



---

**Finding No. 3:**  
**Exception Reporting and Data Exchange Responses**


---

Effective exception reporting procedures allow erroneous or irregular transactions to be identified without disruption of other transactions. The periodic review of exception reports and prompt follow-up on exceptions increase management's assurance that erroneous or fraudulent actions taken through a computer system, should they occur, will be timely detected and corrected.

Our audit disclosed the following exception reporting and data exchange response control deficiencies:

- The Department lacked exception reporting from the FLORIDA System to detect potential employee fraud. The Department created an Internal Controls Workgroup in December 2007 in response to potentially fraudulent Temporary Assistance to Needy Families (TANF) cash assistance payments that we detected during our audit of the State of Florida, Compliance and Internal Controls over Financial Reporting and Federal Awards, audit report No. 2008-141, Finding No. FA 07-046. The Internal Controls Workgroup developed several exception reports, and items on the reports were reviewed for potential fraud. The Internal Controls Workgroup is in the process of developing additional reports and procedures that will dictate who is responsible for reviewing reports and how often the reports will be

reviewed. Without adequate exception reporting, there is an increased risk that erroneous or fraudulent transactions may occur without being detected.

- Although FLORIDA System alerts were generated and on-line reports were implemented to allow ESS staff to monitor data exchange responses, Department reports indicated there were numerous data exchange responses overdue. Data exchange is an electronic sharing of information between the Department and other agencies or systems. The Department performed data exchanges to comply with Federal Income and Eligibility Verification System requirements to validate or identify SSNs, verify receipt of benefits from other sources, verify reported information, and obtain previously unreported information.

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. To assist in ensuring that data exchange responses are processed in a timely manner, the FLORIDA System generated alerts to notify caseworkers when data exchange responses were received by the system and when the caseworkers' actions on the responses were due to be completed. Also, the ESS Program Office had developed data exchange reports that were accessible through its Data and Reports System and were refreshed every morning from FLORIDA System data. The data exchange reports were primarily used by field office staff but were also used by ESS Quality Assurance staff as part of management evaluation reviews. One data exchange report, the Pending Data Exchanges Summary, showed that data exchange responses totaling 728,838 (209,274 of which were responses that were verified upon receipt) were overdue as of January 30, 2008. 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. 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 audit report No. 2008-141, Finding No. FA 07-061.

---

**Recommendation:** The Department should continue its efforts in developing and implementing effective exception reporting procedures. The Department should also address the timely monitoring of data exchange responses.

---



---

**Finding No. 4:**  
**Logging of System Activity**

---

The Department is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which addresses data interchange, privacy, and information security standards for personal health information. According to the HIPAA administrative requirements, a covered entity must ensure the confidentiality, integrity, and availability of all electronic personal health information that it creates, receives, maintains or transmits. Title 45, Section 164.308(a)(1)(ii)(D), Code of Federal Regulations, requires covered entities to implement procedures to regularly review records of information system activity such as logs, access reports, and security incident tracking reports. Logs are critical in monitoring compliance with security policies and investigating security incidents by recording how, when, and by whom certain actions were taken.

The FLORIDA System maintained a log of all updates made to the system. These logs could be viewed on the Case Transaction Activity (IQCT) screen, which shows updates made to a particular case, or the Worker Transaction History (IQWT) screen, which shows updates made by a particular worker. The system, however, did not retain a log of inquiries made of case file information.

The Department Inspector General's Office of Investigations staff stated in certain reports that they were not able to obtain all information necessary from the FLORIDA System to perform their investigations of alleged inappropriate viewing of case file information stored in the system. Although some of the information needed was captured in the system log data set of the Information Management System Transaction Manager, the information was kept for only four calendar days. The system log data set was designed for system recovery but not for system monitoring purposes.

The FLORIDA System contains a large volume of confidential information, including personal health information. Without adequate FLORIDA System logs, there is an increased risk of inappropriate access of confidential information not being detected in a timely manner. Also, without adequate logs to assist in investigations of inappropriate access, the Department's ability to monitor and investigate questionable system activity as provided for in HIPAA may be limited.

---

**Recommendation: The Department should improve FLORIDA System logging to allow for the timely detection of inappropriate or unnecessary access to confidential information, especially personal health information.**

---



---

**Finding No. 5:**  
**Security Controls**

---

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources. Effective security controls include access controls that are intended to ensure that users have only the access privileges needed to perform their duties, that access to sensitive resources is limited to only a few users, and that users are restricted from performing incompatible functions. Access controls include the use of individual user identification codes (IDs) and passwords to allow for attributing user activities to the responsible user. Effective access

controls further include a periodic review to confirm the appropriateness of access rights to help reduce the risk of errors, fraud, misuse, or unauthorized alterations.

Our audit disclosed deficiencies in certain security controls protecting the FLORIDA System and related IT resources. Specifically:

- The Department had implemented procedures to remove the access privileges of employees who terminated employment and contractors whose contracts with the Department had expired. However, while performing access control testing, we identified seven user IDs belonging to five terminated employees and one contractor who had access to FLORIDA System resources from 4 to 964 days after employment termination, which increased the risk of inappropriate use or disclosure of system resources and data. Specifically:
  - One user ID had read-only access privileges to FLORIDA System data sets containing electronic benefits transfer information. This user ID belonged to a former employee who terminated on August 1, 2007. Department staff revoked the access privileges on February 13, 2008, in response to audit inquiry. Department records indicated that the access privileges were used after the employee's termination to view the data sets, which according to Department staff did not contain confidential client information.
  - Four user IDs had access privileges that could have allowed unauthorized disclosure and modification of confidential FLORIDA System data. One of the user IDs had been revoked four days after employee termination. Department staff revoked the access privileges of the other three user IDs on February 6, 2008, in response to audit inquiry. Department records indicated that none of the access privileges associated with the four user IDs were used after the employees' terminations.

- Two user IDs that had access privileges to change FLORIDA System programs and Job Control Language (JCL) belonged to a contractor whose contract with the Department had expired. Although the contractor was no longer under contract with the Department as of December 31, 2007, his access privileges were not revoked until January 25, 2008, because of prolonged contract negotiations. Department records indicated that the last access date field of one of the user IDs was February 11, 2008, or approximately six weeks after the contract expiration date. Our further review of Department records indicated that the last access date field was updated when the user ID was reinstated by the Information Systems Production Services (ISPS) Section Security staff to allow clean-up of data sets associated with the user ID. Department records indicated no activity for either user ID between the contract expiration date and access revocation date.
- Upon audit request, the Department was unable to provide active user access authorization forms for the FLORIDA System specifying the level of access authorized and the user IDs assigned to individuals for 6 of 39 user IDs. Use of standard access authorization forms documents management-approved access privileges and facilitates the periodic monitoring of the appropriateness of access. According to Department staff, forms for 5 of the 6 user IDs had exceeded the Department's two-year record retention policy and the form for the remaining user ID could not be found. Subsequent to audit inquiry, Department staff indicated that new access authorization forms would be created for the user IDs. Without the forms, user accounts in the FLORIDA System could not be readily traced to specific users to determine if their access privileges were appropriate and properly authorized.
- Several groups of computer users within ISPS had unnecessary and excessive access privileges to FLORIDA System computer resources, which increased the risk of inappropriate use or disclosure of system resources and data. Specifically:
  - The Database and Quality and Implementation Control (QIC) groups had the ability to change operating system logs that recorded activities performed on data sets. Database and QIC staff did not require access to operating system logs to perform their job duties. Unnecessary access privileges to change operating system logs increase the risk that unauthorized modifications may be made to the logs, rendering the logs unreliable for use in detecting inappropriate data set access.
  - The QIC group had the ability to change database logs, which was not required for staff in the group to perform their job duties. The database logs recorded all transactions performed in the database. Granting unnecessary access privileges to database logs increases the risk that unauthorized modifications may be made to the logs, rendering the logs unreliable for use in detecting inappropriate transactions.
  - All users in the Mainframe Technical Support group had update access privileges to libraries that contained FLORIDA System production programs and JCL. According to Department staff, it was necessary for some users in the group to have update access privileges to perform systems maintenance, such as creating backups, restoring library contents, and fixing corruption within the library. However, Department staff further indicated that it was not necessary for all users. Unnecessary access privileges to libraries increase the risk of unauthorized modification or destruction of production programs and JCL.
  - The Computer Operations, Scheduling, and QIC groups had the ability to change data in the FLORIDA System outside of normal system edits and controls, which was not appropriate for their job duties. This change ability increases the risk of unauthorized modifications, disclosure, or destruction of confidential FLORIDA System data.

- Within the FLORIDA System, access to perform security administration functions and view confidential information was not adequately restricted based on functional and organizational requirements, which increased the risk of unauthorized modification, disclosure, loss, or impairment of FLORIDA System resources and data. Specifically:
- When the FLORIDA System was designed, various public assistance programs and the Child Support Enforcement Program were the responsibility of the Department. Subsequently, the Child Support Enforcement Program was transferred to the Department of Revenue (DOR). Because of the original design of the system, users within the Department and DOR had access privileges to perform FLORIDA System security administration functions that crossed department boundaries. Security administrators at the Department and at DOR continued to be able to add, modify, or delete access for all FLORIDA System users regardless of the department for which the user worked. Functionally, the security administrators were only responsible for security administration within their respective departments, making cross-departmental security administration privileges unnecessary and excessive. There were 616 user IDs from both departments that provided the capability to view the SSNs of employees of both departments. These 616 user IDs were associated with 507 individual users and 27 generic IDs. On February 19, 2007, the Department issued a programming change request to correct this access control deficiency. According to Department staff, this change was implemented in March 2008.
  - Additionally, during access control testing, we identified one DOR employee who was assigned to the Data Security Group in Resource Access Control Facility (RACF). This assignment granted the employee excessive access privileges to security administration functions and computer hardware logs for the FLORIDA System that were not necessary in the performance of the employee's job duties. In response to audit inquiry, Department staff removed Data Security Group access privileges for the DOR employee on February 14, 2008.
- Additional access control deficiencies existed in the FLORIDA System, the specific details of which are not disclosed in this report to avoid the possibility of compromising the Department's IT security controls. However, appropriate Department personnel have been notified of the deficiencies, which are summarized below.
- Group user IDs were being used to manage some of the Department's network resources. Additionally, password controls related to these group user IDs needed improvement. The absence of strong user ID and password controls whereby each user is assigned a unique user ID and password increases the risk that the Department will not be able to trace user activities to the responsible individual. Also, by not maintaining adequate password controls, the risk is increased that access violations may occur and not be detected in a timely manner.
  - Network barrier and transmission controls needed improvement to reduce the risk of unauthorized use of the Department's networks and systems.

---

**Recommendation: The Department should perform a periodic review of access privileges to ensure terminated user access is revoked and that access privileges to computer resources is appropriate. The Department should also ensure that user access authorization forms are appropriately maintained. Additionally, the Department should improve security administration within the FLORIDA System, strengthen user ID and password controls, and ensure that appropriate network barrier and transmission controls are in place.**

---

**Finding No. 6:****ISM Organizational Placement**

Section 282.318(2)(a)1., Florida Statutes, provides that each agency head shall designate an ISM who shall administer the security program of the agency for its data and IT resources. Placement of the ISM at a sufficiently high level within the organizational structure helps promote the effectiveness of the information security function by:

- Separating the information security function from other organizational units, thereby maximizing its independence and objectivity.
- Enabling sufficient authority to coordinate risk management activities and monitor compliance with security policies and procedures, throughout the agency.
- Providing an appropriate profile with senior management to facilitate reporting and making recommendations to senior management regarding risk management and security issues.
- Emphasizing the importance of information security.

At the Department, the organizational placement of the ISM and the information security function was not at a sufficiently high level to maximize the effectiveness of the information security function or reflect an appropriate level of importance and priority of security within the Department. The ISM and the information security function were located administratively in the Central Office within ISPS. Security duties were performed by staff within the Central Office and the five Regional Program Offices. Each of the regions had security officers and coordinators. The ISM was responsible for administration and coordination of the data processing personnel who were responsible for planning, developing, and coordinating the Department's information security program.

However, even though the ISM coordinated reports of the Regional Program Offices' security awareness training, risk assessments, and other activities, the ISM did not have oversight responsibilities, contrary to

Section 282.318(2)(a)1., Florida Statutes, over the Regional Program Offices to ensure that security policies and procedures were being followed. In addition, contrary to Section 282.318(2)(a)1., Florida Statutes, the ISM was not adequately involved in the implementation of application-level security administration for the FLORIDA System. Specifically, the ISM did not provide oversight to ensure that application-level security administration was in compliance with Department policies and procedures, such as provisions for enforcement of separation of duties as previously discussed in Finding No. 2. Because the ISM and the information security function reported to an IT operational function, its independence and effectiveness would be enhanced through placement at a higher level within the Department.

The lack of oversight capability, appropriate independence, and sufficient authority required by the ISM to administer the information security program at a Departmentwide level may limit the effectiveness of security over the Department's information resources and provide insufficient emphasis of the importance of information security to management. Additionally, the lack of an appropriately placed ISM with sufficiently defined authority and responsibility may have contributed to the issues discussed in Finding Nos. 1, 2, 5, and 7 of this report.

---

**Recommendation:** The Department should review the organizational placement of the information security function and the ISM and reposition the information security function to strengthen its independence and authority and further emphasize the importance of security within the Department. The ISM should be given proper authority over Regional security officers and provide oversight of security administration within Department systems.

---

**Finding No. 7:****Risk Management Procedures**

An effective information security program includes risk management procedures that identify, assess, and reduce IT-related risks to an acceptable level. Our audit disclosed aspects of the Department's risk management procedures that needed improvement. Specifically:

- The Department's standard operating procedures for IT risk management were not up to date. The standard operating procedures were last updated on August 10, 2000, and contained references to positions and systems that were obsolete or never implemented. Absent current risk management procedures, the risk is increased that security risks to the Department's data and IT resources will not be effectively addressed and mitigated.
- The Department's risk management procedures were deficient in other areas, increasing the risk that security vulnerabilities will not be timely detected. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising the Department's IT security controls. However, appropriate Department personnel have been notified of these deficiencies.

---

**Recommendation: The Department should update and improve its risk management procedures to reflect the current IT environment and enhance its ability to detect security vulnerabilities in a timely manner.**

---

**Finding No. 8:****Systems Development and Modification Controls**

Systems development and modification controls help ensure that only authorized programs and authorized modifications are implemented. The continued integrity of programs is protected by instituting policies, procedures, and techniques that help ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled.

Our audit disclosed instances of missing or outdated systems development and modification procedures and control practices that needed improvement. Specifically:

- The Department's information systems development methodology (ISDM), last updated on August 23, 1994, was superseded by a standard operating procedure that was approved on October 21, 2000, and contained references to positions that no longer existed and processes and software that were never implemented. Without a documented ISDM, there is an increased risk that control activities over the systems development life cycle will not be carried out as management intended.
- Server application change management procedures were out of date and did not reflect the current processes used by the Department. Without updated change management procedures, control activities may not be consistently applied resulting in unauthorized program changes.
- Procedures were not documented for the appropriate use of an internal ID code for Endeavor, the software used to control and monitor the development and implementation of mainframe programs. QIC staff who were responsible for moving mainframe programs into production had access to an internal Endeavor ID code that could be used to perform various tasks, such as archiving programs. During testing of FLORIDA System change controls, we noted that some programs were moved into production using the Endeavor ID code. This was the result of a QIC staff member not removing the Endeavor ID code from his job card. In response to audit inquiry, Department staff stated that the internal Endeavor ID code was limited to QIC staff and it was appropriate for QIC staff to use the ID code. However, any activity performed in Endeavor using the internal Endeavor 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 Endeavor, should they occur.

- The Department did not have written procedures for the deployment and configuration of macros, which are programming language statements that perform sequences of computer instructions. Without documented procedures, there is an increased risk of inappropriate or unauthorized macros being implemented.

---

---

**Recommendation: The Department should ensure that all systems development and modification procedures are up to date and reflect appropriate control activities.**

---

---

---

---

#### **PRIOR AUDIT FINDINGS**

---

---

Finding Nos. 1, 2, 6, and 8 above include issues repeated from audit report No. 2005-106. Other IT deficiencies noted in the prior audit that were within the scope of this audit have been corrected or were in the process of being corrected.

---

---

#### **OBJECTIVES, SCOPE, AND METHODOLOGY**

---

---

The objectives of this IT audit were to determine the effectiveness of selected general and application controls related to the FLORIDA System and to determine whether the Department had corrected, or was in the process of correcting, selected deficiencies disclosed in audit report No. 2005-106, Finding Nos. 1 through 6.

The scope of our audit focused on evaluating selected IT controls applicable to the FLORIDA System and selected interfacing ESS systems during the period October 2007 through March 2008, with selected actions taken from July 1, 2006.

This IT audit was conducted in accordance with Generally Accepted Government Auditing Standards. In conducting our audit, we interviewed appropriate Department personnel, reviewed policies and procedures and other applicable documentation, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to the FLORIDA System.

**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 audit.



David W. Martin, CPA  
Auditor General

**MANAGEMENT RESPONSE**

In a letter dated June 25, 2008, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

This audit was conducted by Gwen Pacubas and supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, via e-mail at [joningram@aud.state.fl.us](mailto:joningram@aud.state.fl.us) or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.myflorida.com/audgen/>); by telephone (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

**APPENDIX A**  
**MANAGEMENT RESPONSE**



**State of Florida**  
**Department of Children and Families**

**Charlie Crist**  
*Governor*

**Robert A. Butterworth**  
*Secretary*

---

June 25, 2008

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

Dear Mr. Martin:

Thank you for your May 27 letter accompanying the preliminary and tentative findings of the *Information Technology Audit of the Department of Children and Family Services, Florida On-Line Recipient Integrated Data Access System*.

The Department concurs with all of the recommendations of your report, and we are currently working to address them. If you or your staff have additional questions, please feel free to call Ms. Melissa Jaacks, Assistant Secretary for Administration, at (850) 488-6062.

Sincerely,

A handwritten signature in black ink, appearing to read "Rob Butterworth", is written over a printed name and title.

Robert A. Butterworth  
Secretary

---

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