State of Florida
Department of Children and Families

Charlie Crist
Governor

George H. Sheldon
Secretary

DATE: July 19, 2010

TO: George H. Sheldon
Secretary

FROM: Jason Dimitris
Interim Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2010-066

In accordance with Section 20.055(5)(g), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2010-066, "*Florida Department of Children and Family Services, Florida On-Line Recipient Integrated Data Access System (FLORIDA), Information Technology Audit.*"

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

Enclosures

cc: Kathy DuBose, Staff Director, Joint Legislative Auditing Committee

DEPARTMENT OF CHILDREN AND FAMILIES

OFFICE OF INSPECTOR GENERAL

George H. Sheldon
Secretary

Enhancing Public Trust in Government

Jason Emilios Dimitris
Interim Inspector General

Project #E–0910-016

July 16, 2010

Six-Month Status Report
Department of Children and Family Services Florida Online Recipient Integrated Data Access (FLORIDA) System, Information Technology Operational Audit

PURPOSE

The purpose of this report is to provide a written response to the Secretary on the status of corrective actions taken six months after the Auditor General published Report No. 2010-066 *Department of Children and Family Services* – Florida Online Recipient Integrated Data Access (FLORIDA) System, Information Technology Operational Audit.

REPORT FINDINGS, COMMENTS & STATUS

The Department was responsible for providing updated status and corrective action comments for findings one through twelve. Presented below are the full text of the Auditor General's recommendations and up-to-date corrective action comments and status for audit findings, as reported by the Information Technology Services (ITS) staff.

RECOMMENDATION #1: *The Department should comply with State law by clearly establishing why the use of employee Social Security Numbers (SSNs) is imperative for the Department to perform its duties and responsibilities or alternatively establish another number to be used rather than the SSN.*

Status (per Information Technology Services staff): Completed

The PRIVACY ACT STATEMENT at the bottom of the Security Agreement Form states the imperative need for the use of SSN. 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.

RECOMMENDATION #2: *The Department should enhance the effectiveness of FLORIDA System controls to enforce an appropriate separation of case management duties.*

Status (per Information Technology Services staff): Completed

The Office of Internal Audit removed the corrective action comments due to the technical – security concern and hand-delivered them to Auditor General staff.

RECOMMENDATION #3: *The Department should continue to seek solutions for ensuring that data exchange responses are processed within the required time frames.*

Status (per Information Technology Services staff): Ongoing

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 ITS 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 Supplemental Nutrition Assistance Program (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 complete this work due to limited programming staff.

RECOMMENDATION #4: *The Department should improve FLORIDA System Public Assistance (PA) Component user account management procedures by ensuring that access authorization forms are appropriately completed and maintained.*

Status (per Information Technology Services staff): In-process

The Department will develop a refresher course on FLORIDA security controls. This work is currently planned to be completed in December 2010.

RECOMMENDATION #5: *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.*

Status (per Information Technology Services staff): Completed

The Department will continue to remind supervisors to notify their local security officer when employees leave the Department. This process will also be included as a component of the refresher training that is provided to security officers.

RECOMMENDATION #6: *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.*

Status (per Information Technology Services staff): In-process

The Department will develop a refresher course on FLORIDA security controls. This work is currently planned to be completed in December 2010.

RECOMMENDATION #7: *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.*

Status (per Information Technology Services staff): On-going

The Department has started sending out a security access list to all security officers for their review. This list goes out every month.

RECOMMENDATION #8: *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.*

Status (per Information Technology Services staff): In-process

The Department has implemented processes that will help ensure that badge authorization forms are updated when access changes are made. The Department conducted a joint Photo ID Badge Audit (performed by both the Department and the Northwood Shared Resource Center) where all badges with access to the Northwood Shared Resource Center Computer Room were reviewed. This audit was completed in early January 2010. As a result of the audit, the number of individuals with access to the computer room was reduced significantly. The Department is in the process of conducting a second Photo ID Badge Audit at this time. The Department is comparing all Badge Authorization Forms to the access that individuals actually have in the Badge System to ensure that the individuals have the access approved in the forms. The audit is 95 percent complete and should be completed by July 31, 2010.

RECOMMENDATION #9: *The Department should improve password and network barrier and transmission controls to ensure the confidentiality, integrity, and availability of data and IT resources.*

Status (per Information Technology Services staff): Completed

The Department will improve password and network controls. The Department has implemented Microsoft Active Directory Complex Passwords standards. The passwords must be eight characters and have three of the following four types of characters: numbers, upper case, lower case, or special characters. No portion of the Log-in Name can be used in the password.

RECOMMENDATION #10: *The Department should establish a written Systems Development Life Cycle (SDLC) methodology and ensure that all systems development and modification policies and procedures are up to date and reflect appropriate control activities.*

Status (per Information Technology Services staff): In-Process

The Department is in the process of updating System Development and Modification Procedures.

RECOMMENDATION #11: *The Department should ensure that its programming change control policies are followed and that program changes are appropriately documented in the program modification logs.*

Status (per Information Technology Services staff): Completed

The Department has made changes to the Change Management Process to ensure that all program changes are reviewed to verify that the modification logs are documented prior to the change moving forward to Acceptance and Production. The Department has implemented an approval process so that the code changes are not approved and promoted through the software development life cycle without the proper modification logs.

RECOMMENDATION #12: *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.*

Status (per Information Technology Services staff): Completed

The Office of Internal Audit removed the corrective action comments due to the technical – security concern and hand-delivered them to Auditor General staff.

This follow-up audit was conducted as required by Florida Statute 20.055(3)(g) and section 2500.A1 of the International Standards for the Professional Practice of Internal Auditing as published by the Institute of Internal Auditors. Elton Jones compiled this follow-up audit from representations provided by program management. Please address inquiries regarding this report to Jerry Chesnutt, Director of Auditing, at (850) 488-8722.