State of Florida
Department of Children and Families

Rick Scott
Governor

David E. Wilkins
Secretary

DATE: October 5, 2011

TO: David E. Wilkins
Secretary

FROM: Dawn E. Case
Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2011-141

In accordance with Section 20.055(5)(h), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2011-141, "Florida Department of Children and Family Services, Florida On-Line Recipient Integrated Data Access System (FLORIDA), Information Technology Operational Audit."

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

Enclosure

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 Dimitris
Interim Inspector General

Project #E-1011DCF-035

October 5, 2011

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. 2011-141 *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 eight. 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: *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.*

Status (per Information Technology Services staff): Partially Completed

Although by no means are we suggesting that we will be able to completely discontinue the practice of using SSN (until such time as a complete system re-write occurs), beginning in October 2011 we propose to revisit the feasibility of using an alternate unique identifier and provide findings to executive management by January 2012.

RECOMMENDATION #2: *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): Partially Completed

Our efforts (listed below and as our response to the preliminary and tentative findings) are sufficient for compliance and remaining efforts are supervisory issues associated with the operational departments. More definitive direction would have to be provided for any remaining deficiencies.

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. 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). Data exchanges are posted as we receive them. 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.

RECOMMENDATION #3: *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.*

Status (per Information Technology Services staff): Ongoing

We will continue to periodically audit and continuously train regional and headquarters security officers to ensure authorizations are properly documented. The Department's Security Awareness Training's content and design has been notably improved and the Security Awareness Training is required as a part of an annual training curriculum required of all DCF employees. Internal controls have been implemented to ensure only proper authorization is granted to individuals entrusted with viewing ACCESS FLORIDA system information.

Additionally, the FLORIDA team has prepared additional training for the regional and facility Information Systems Security Officers which is available for review and the training will become the foundation for a new FLORIDA System User Account Management Procedure.

RECOMMENDATION #4: *The Department should ensure that the access privileges of former employees are disabled in a timely manner pursuant to the FLORIDA Security Guide.*

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

Department of Children and Families Services has improved procedures to disable non-user accounts within 24 hours of separation from employment via direct reporting from Human Resources to our identity management team. (See CFOP 60-70, EMPLOYEE SEPARATIONS AND REFERENCE CHECKS, §b.(4.). Also, see page 4 for form notification.)

DCF will continue to reinforce the existing policy to remove access to the applications, network and facilities upon the time of termination.

The system automatically disables accounts after 45 days of inactivity. After 90 days, the accounts are revoked from the system. Furthermore, on a monthly basis, the security officers receive a report indicating discrepancies in the users listed in RACF and the application's security system (SMUM). Using this report, the security officers are responsible for taking action if needed to resolve the discrepancies.

RECOMMENDATION #5: *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.*

Status (per Information Technology Services staff): Completed

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. Our efforts are sufficient for compliance and we continue efforts at monitoring least privileged access. More definitive direction will have to be provided for any remaining deficiencies.

RECOMMENDATION #6: *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.*

Status (per Information Technology Services staff): Partially Completed

In the past two years, two complete audits of photo ID badges have been accomplished and audits will continue to be conducted annually. As a result of the audits, the number of individuals with access to the computer room was reduced significantly and rules put into place that systematically disables badge access after 45-days of non-use. The most recent audit verified Badge Authorization Forms permissions to the individual access permissions in the Badge System to ensure that the individuals have only the access approved in the forms. This audit was completed in August 2011.

A Northwood Photo-ID Badge procedure has been drafted and is available for review that includes provisions for the life-cycle management of Northwood facility badges and includes provisions for the annual audit of photo-id badges. This procedure is being reviewed by management and is scheduled to be published in November 2011.

RECOMMENDATION #7: *The Department should improve password controls to ensure the confidentiality, integrity, and availability of data and IT resources.*

Status (per Information Technology Services staff): Completed

We have implemented Microsoft Active Directory Complex Passwords standards. The passwords must be 8 characters and have 3 of the following 4 characters types: Numbers, Upper Case Characters, Lower Case Characters, or Special Characters. Another restriction is that the user can't use any portion of the Login Name in the password.

DCF completed a conversion to SonicWall-Aventail, an LDAP based authentication VPN, replacing the NetMotion VPN system. SonicWall-Aventail has higher level encryption capability than NetMotion, requires individual names user authentication, performs logging of activity and requires password changes every 45 days.

RECOMMENDATION #8: *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.*

Status (per Information Technology Services staff): Completed

The FLORIDA Change Management Guide has been updated and posted to the Intranet site. As an SDLC for the FLORIDA system in production today, the change control guide will undergo review for any modifications necessary to accurately represent existing sustaining engineering processes for all FLORIDA development teams.

This follow-up audit was conducted as required by Florida Statute 20.055(5)(h) 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.