State of Florida
Department of Children and Families

Charlie Crist
Governor

George H. Sheldon
Secretary

DATE: February 12, 2009

TO: George H. Sheldon
Secretary

FROM: Sheryl G. Steckler
Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2008-197

In accordance with Section 20.055(5)(g), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2008-197, "*Florida Department of Children and Family Services, Florida On-Line Recipient Integrated Data Access System, Information Technology Audit.*"

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

Enclosure

cc: Terry Shoffstall, Staff Director, Joint Legislative Auditing Committee

DEPARTMENT OF CHILDREN AND FAMILIES

OFFICE OF INSPECTOR GENERAL

George H. Sheldon
Secretary

Sheryl G. Steckler
Inspector General

Report #E-19-0708-096

February 12, 2009

SIX-MONTH STATUS REPORT
AUDITOR GENERAL REPORT #2008-197
Florida Department of Children and Family Services
Florida On-Line Recipient Integrated Data Access System
Information Technology Audit

PURPOSE

This report provides a written response to the Secretary on the status of corrective actions taken six months after the Florida Auditor General published report number 2008-197, *"Florida Department of Children and Family Services, Florida On-Line Recipient Integrated Data Access System, Information Technology Audit."*

REPORT FINDINGS, COMMENTS & STATUS

Presented below are the up-to-date corrective action comments and status for audit findings 1 through 8, as reported by the Office of Information Technology Services (IS) staff.

RECOMMENDATION #1: *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.*

Status per Information Technology Services staff: (Pending)

Information Technology Services and Legal Services will work together to further justify why the use of SSN is imperative.

RECOMMENDATION #2: *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.*

Status per Information Technology Services staff: (Complete)

The FIAT process is one way of requesting and authorizing benefits on FLORIDA. The SSN edit was already in place in the other areas of benefit request and authorization. In May 2008, we programmed the FLORIDA system so that a user with multiple user IDs and the same SSN can not **request** and **approve** benefits using the FIAT process.

RECOMMENDATION #3: *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.*

Status per Information Technology Services staff: (Ongoing)

IS works with ACCESS to implement program policy.

EXCEPTION REPORTING - In December 2007, ACCESS formed an Internal Controls Workgroup to combat employee fraud. As a result, based on areas the workgroup identified as possible avenues for employee fraud, several data reports were designed to monitor employees' actions. Part of this workgroup, which consists of individuals with program and policy knowledge and fraud prevention expertise, reviews these reports monthly for irregularities. The entire group meets monthly to discuss the results of the data reviews, improvements, or refinements to the reports.

In addition to the monthly meetings, in May 2008, ACCESS initiated an Employee Fraud Taskforce, which consists of the Internal Controls Workgroup and representatives from the Office of Inspector General, and the Director of the Florida Department of Law Enforcement's Public Assistance Fraud unit. This group meets quarterly to review and share trends discovered as a result of any public assistance fraud investigations conducted by their offices and any additions/improvements that need to be made to our current data reports.

DATA EXCHANGES – Our ACCESS Data and Reports System provides daily updates for all data exchanges that have been processed and those that are unreviewed. Local unit supervisors of the Case Maintenance Units monitor these reports on a regular basis for timeliness and accuracy.

Additionally, the FLORIDA system is programmed to automatically update assistance groups with income information (verified upon receipt) from data exchanges. Social Security or Supplemental Security Income changes are examples of automatic updates.

RECOMMENDATION #4: *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.*

Status per Information Technology Services staff: (Complete)

IS works with ACCESS to implement program policy. Starting October 28, 2008, we store the FLORIDA inquiry audit trail information for one year. We also store update information indefinitely. The ACCESS Internal Control Workgroup routinely uses the FLORIDA logs for identifying alleged fraud cases. We have completed enhancements to the FLORIDA system to capture and store FLORIDA screen data when National Directory New Hire (NDNH) or Office of Vital Statistics (OVS) data has been accessed.

RECOMMENDATION #5: *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.*

Status per Information Technology Services staff: (Complete and Ongoing)

Information Technology Services is performing periodic reviews of access privileges to validate that access is appropriate.

Information Technology Services has also created individual userIDs on the Department's network resources, where technically feasible.

RECOMMENDATION #6 *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.*

Status per Information Technology Services staff: (Complete)

The ISM now reports directly to the Chief Information Officer (CIO). Although the ISM has authority for Department security, there are no plans to change the organizational structure at this time.

RECOMMENDATION #7: *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.*

Status per Information Technology Services staff): (Ongoing)

These procedures are reviewed and updated periodically.

RECOMMENDATION #8: *The Department should ensure that all systems development and modification procedures are up to date and reflect appropriate control activities.*

Status per Information Technology Services staff: (Ongoing)

Information Systems is continually updating and refining the development and modification procedures to ensure proper controls are in place.

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.