State of Florida
Department of Children and Families

Rick Scott
Governor

Esther Jacobo
Interim Secretary

DATE: November 22, 2013

TO: Esther Jacobo
Interim Secretary

FROM: Keith R. Parks
Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2013-005

In accordance with Section 20.055(5)(h), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2013-005, *"Department of Children and Family Services, Florida Online Recipient Integrated Data Access (FLORIDA) System, Information Technology Operational Audit."*

The Office of Internal Audit compiled these up-to-date corrective action representations to resolve findings, as reported by program management.

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

MYFLFAMILIES.COM

OFFICE OF INSPECTOR GENERAL

Esther Jacobo
Interim Secretary

Enhancing Public Trust in Government

Keith R. Parks
Inspector General

Project #E-1112DCF-080

November 22, 2013

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. 2013-005, *Department of Children and Family Services, Florida Online Recipient Integrated Data Access (FLORIDA) System, Information Technology Operational Audit.*

REPORT FINDINGS, RECOMMENDATIONS, STATUS & COMMENTS

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 finding statements and recommendations and up-to-date corrective action comments and status, as reported by the Information Technology Services (ITS) staff.

***FINDING NO. 1**: Contrary to Section 119.071(5)(a)2.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. 2011-141.*

***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 in the FLORIDA System rather than the SSN.*

Status (per Information Technology Services staff): Pending

The Department completed the analysis and estimation of costs associated with establishing another number to be used in the FLORIDA System rather than the Social Security Number. The Department is targeting to complete the changes required to establish an alternate number in State Fiscal Year 2014 - 2015. A final decision on funding the associated costs for the changes through submission of a legislative budget request, or through allocation of Fiscal Year 2014 - 2015 FLORIDA System maintenance and operational funds is under Department consideration.

***FINDING NO. 2:** As similarly noted in our report No. 2010-066, FLORIDA System edits designed to prevent employees from performing incompatible case management functions could be circumvented in certain instances.*

***RECOMMENDATION:** The Department should take steps to minimize the likelihood that the FLORIDA System edit enforcing an appropriate separation of case management duties could be circumvented.*

Status (per Information Technology Services staff): Fully Corrected

Functionality/edits to prevent workers from creating and approving the same benefit are done by validating that the workers are in fact different. This is done in a behind the scenes comparison of SSNs. When security officers incorrectly enter the SSN, the edits are circumvented. To minimize the likelihood that the FLORIDA System edits enforcing an appropriate separation of case management duties can be circumvented, the Department has instructed the security officers to conduct a quality review and re-check the SSNs before submission.

FINDING NO. 3: *The Department had numerous unprocessed overdue data exchange responses. Similar findings were noted in prior audits of the Department, most recently our report No. 2011-167, Finding FA 10-064, and report No. 2011-141.*

RECOMMENDATION: *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): Fully Corrected

The system enhancement design was completed and installed on December 12, 2012. Through its quality assurance efforts, the ACCESS Office of Quality Management monitors Data Exchanges in accordance with the priority policy guidance to ensure they are processed timely and accurately and requires corrective action, where necessary.

FINDING NO. 4: *As similarly noted in prior audits of the Department, most recently our report No. 2011-141, documentation of authorization for the FLORIDA System PA Component access privileges of some employees was missing, incomplete, or inaccurate.*

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.

Status (per Information Technology Services staff): Partially Corrected

The Department will improve its FLORIDA System PA Component user account management procedures by:

- Updating procedures that will outline how forms are to be accurately completed and standardize how forms are maintained.
- Creating a procedure to take a random sampling of access authorization forms from each regional office and headquarters semi-annually to ensure policy guidelines on completion, accuracy, and maintenance are being followed. A formal report will be developed for management on findings that do not comply with the developed policy and procedures for access authorization forms.
- Creating a secured location within the Department network for all access authorization forms to be stored electronically.

All of these tasks will be completed and updated in policy. The policy has an anticipated completion date of December 31, 2013.

FINDING NO. 5: *The IT resource access privileges of some mainframe technical support staff and groups exceeded what was necessary for their job duties. Similar findings were noted in prior audits of the Department, most recently our report Nos. 2010-066 and 2011-141.*

RECOMMENDATION: *The Department should remove the unnecessary and excessive access privileges and review the ongoing appropriateness of all access privileges granted to the FLORIDA System production datasets to ensure that access is commensurate with the requirements of employee job duties and to ensure the reliability of the above-described FLORIDA System IT resources.*

Status (per Information Technology Services staff): Fully Corrected

The Department performed a review of the Northwood Shared Resource Center (NSRC) mainframe technical support staff access. Access privileges for NSRC technical staff have been updated to remove any unnecessary and excessive access privileges.

FINDING NO. 6: *As similarly noted in prior audits of the Department, most recently our report No. 2011-141, the Department did not timely deactivate the PA Component access privileges of some former employees.*

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

Status (per Information Technology Services staff): Fully Corrected

The Department worked with its own Human Resources group to establish a termination file that is sent to the regional and headquarters' security officer. This file is automatically generated from People First and contains a listing of employees that separated from the Department. The Department's security officers have been instructed to use this file to terminate FLORIDA System access for individuals listed. This file is sent to the security officers on a daily basis.

- As a compensating control, the FLORIDA System automatically revokes the Resource Access Control Facility (RACF) account for the user after 45 days of inactivity. The FLORIDA system has been modified to send a monthly SMUM/RACF Reconciliation report to the security officers to ensure that any discrepancies between SMUM and RACF are resolved timely. RACF revokes user 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.

FINDING NO. 7: *Certain Department security controls related to passwords and the transmission of FLORIDA System information needed improvement. Similar findings related to passwords were noted in prior audits of the Department, most recently our report No. 2011-141.*

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

Status (per Information Technology Services staff): Fully Corrected

All 3,270 terminal emulation sessions were modified to secure session. From that point forward, all requests and downloads from the BlueZone server are "secure session only." As of September 2012, FLORIDA System (RACF) password requirements were lengthened from 6 to 8 characters to provide additional security controls.

FINDING NO. 8: *As similarly noted in prior audits of the Department, most recently our report No. 2011-141, the Department's systems development and modification policies and procedures needed improvement.*

RECOMMENDATION: *The Department should establish a written systems development life cycle (SDLC) methodology that details the procedures that are to be followed when systems and applications are designed, developed, and subsequently modified.*

Status (per Information Technology Services staff): Fully Corrected

An SDLC policy (SOP SDLC No. 50-17) was developed and posted on the Intranet on January 9, 2013.

This follow-up audit was conducted as required by Florida Statutes 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.