MYFLFAMILIES.COM

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Interim Secretary

DATE: October 27, 2014

TO: Mike Carroll
Interim Secretary

FROM: Keith R. Parks
Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2014-188

In accordance with Section 20.055(5)(h), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2014-188, *Domestic Violence Program, Telework Program, and Selected Administrative Activities, 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

MYFLFAMILIES.COM

OFFICE OF INSPECTOR GENERAL

Mike Carroll
Interim Secretary

Enhancing Public Trust in Government

Keith R. Parks
Inspector General

Project #E-1213DCF-140

October 27, 2014

Six-Month Status Report

DEPARTMENT OF CHILDREN AND FAMILIES DOMESTIC VIOLENCE PROGRAM, TELEWORK PROGRAM, AND SELECTED ADMINISTRATIVE ACTIVITIES 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. 2014-188, *Domestic Violence Program, Telework Program, and Selected Administrative Activities, Operational Audit.*

REPORT FINDINGS, RECOMMENDATIONS, STATUS & COMMENTS

The Offices of Domestic Violence, Contracted Client Services, Human Resources, Information Technology Services, and Financial Management Services collectively provided updated status and corrective action comments to the findings and recommendations. 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 management staff of the aforementioned programs.

FINDING NO. 1: *Department monitoring of the Florida Coalition Against Domestic Violence (Coalition) was not always properly documented or sufficient to ensure that the Coalition complied with contractual terms and applicable State laws and Federal regulations.*

RECOMMENDATION: *We recommend that Department management strengthen contract monitoring policies and procedures to ensure that: monitoring of contract provider fiscal activities is performed, supervisory reviews of the monitor's work are conducted and documented, and the conclusions made during desk reviews are adequately supported. Additionally, we recommend that Department management ensure that when monitoring the Coalition, the allocation of funds to the domestic violence centers be addressed.*

Status (per Offices of Domestic Violence and Contracted Client Services staff): Partially Corrected

The Department has completed the redesign of the desk review process and addressed requirements for quality assurance by monitoring team leaders at a statewide meeting and monitoring staff training in July 2014. The monitoring policy is being updated. The Department continues to consider the extent to which its approach to fiscal monitoring may change.

FINDING NO. 2: *The Department could not provide written telework agreements for some employees participating in the Department's Telework Program. Additionally, teleworkers' performance evaluations did not always include required notations to evidence the continuing appropriateness of the telework arrangements.*

RECOMMENDATION: *We recommend that the Department's Office of Human Resources staff continue to communicate to appropriate supervisory staff the requirements outlined in Department policies and procedures to help ensure that telework agreements are executed and that decisions to continue teleworking arrangements are properly documented in the employees' annual performance evaluations.*

Status (per Office of Human Resources staff): Fully Corrected

Department leadership was advised of requirements via written communication dated July 7, 2014. The Office of Human Resources also met with key leaders in the Department and emphasized the need to ensure these recommendations are implemented.

FINDING NO. 3: *The Department did not always document the assignment and return of laptop computers for teleworking employees. Additionally, Department policies and procedures were not sufficient to ensure that terminated or transferred Telework Program employees' laptop and desktop computers were timely sanitized to remove sensitive data or that documentation of the sanitization was maintained.*

RECOMMENDATION: *We recommend that Department management update policies and procedures to include a required time frame for sanitizing the computer equipment returned by Department staff. In addition, we recommend that Department management continue to emphasize to staff the requirements for documenting the assignment, custody, and sanitization of computer equipment.*

Status (per Office of Information Technology Services staff): In Progress

The Office of General Services will work with the Office of Information Technology Services and the Regions to determine a reasonable timeframe for sanitizing the computer equipment returned by teleworking employees. Hard drive crushers and duplicators have been purchased and distributed to facilitate the timely sanitization of hard drives. Once a reasonable timeframe has been determined, the Office of General Services will work with the Office of Human Resources to update the appropriate policies and procedures for documenting the assignment and return of laptop computers for teleworking employees, and for the timely sanitization of laptop and desktop computers.

FINDING NO. 4: *The Department did not always properly document the timely review of teleworker background screening results and, in some instances, the dates that fingerprints were submitted for background screenings were inaccurately recorded in People First.*

RECOMMENDATION: *We recommend that Department management ensure that background screening coordinators timely issue and place background screening clearance letters or other equivalent documentation in the applicable employee personnel files, in accordance with Department policies and procedures. We also recommend that Department management update policies and procedures to provide specific written instruction for entering in People First the dates fingerprints are submitted and background screenings are completed.*

Status (per Office of Human Resources staff): Fully Corrected

As noted on pages 17-18 of Report No. 2014-188, a process change that has occurred with implementation of Human Resources Shared Services (HRSS) is the use of an Appointment Checklist, which includes a background screening clearance block. The HRSS Center will not process an employee appointment and put an employee on the payroll unless the selected applicant's background screening has been cleared. The Appointment Checklist includes the Date Submitted and Date Completed. The completed Appointment Checklist is incorporated into the employee's personnel file. The Appointment Checklist constitutes equivalent documentation of background screening clearance, and documents that the selected applicant cleared the background screening process.

Office of Human Resources staff have been provided instructions in our Desk Reference Guide (DRG) for entering dates related to background screening and fingerprinting.

Instructions require the use of the Appointment Checklist within the hiring package to update the Background Screening in the People First System by following the procedures below.

- To enter Background Screening Dates, click "Work Information Maintenance."
- Click "Fingerprints" for background screening information.
- Click "new."
- Enter date submitted (sent for fingerprints) and completed (clearance provided) in mm/dd/yyyy format.
- Enter end date. End date will be five years from submission date.
- Click "save."
- Click "menu."

FINDING NO. 5: *The Department had not established policies and procedures for the collection and use of social security numbers (SSNs) or evaluated its collection and use of SSNs to ensure compliance with State law.*

RECOMMENDATION: *We recommend that Department management establish written policies and procedures regarding the collection and use of individuals' SSNs, timely finalize the review of the Department-wide survey of SSN collection activities, and take appropriate steps to demonstrate compliance with applicable statutory requirements.*

Status (per Office of Information Technology Services staff): In progress

The Office of Administrative Services will work with the program areas to take the necessary steps to demonstrate compliance with applicable statutory requirements and establish policies and procedures for the collection and use of SSNs. An update for the five applicable Information Technology systems is below.

(1) Florida Online Recipient Integrated Data Access (FLORIDA) System: Due to the scope and cost associated with the changes required to eliminate SSNs in this component of the FLORIDA System, the Department has made the decision to incorporate replacement of these functions into a legislative funding request that seeks funds to replace all legacy components of the FLORIDA System. As of October 2014, a Legislative Budget Request (LBR) was created and approved to move forward by Department Executive Management. The LBR seeks FY 2015/2016 funds to initiate the work necessary to complete the replacement of remaining FLORIDA System legacy functions and components. In addition, the legislatively mandated feasibility study supporting the request has been drafted.

The outcome of the review of this LBR and the results of legislative action to approve and fund the Department's request will determine the timing for replacement of this SSN dependent function in the FLORIDA System.

(2) Information Delivery System Query Facility: This is a "read only" information data warehouse system that collects information from the Department of Financial Services' Florida Accounting Information Resource Subsystem (FLAIR) and is used for reporting purposes. Documents contained in this application are due to the requirement of the Department of Financial Services.

(3) Florida Safe Families Network (FSFN): In conjunction with the Office of Child Welfare, Family and Community Services Information Technology staff is facilitating an access control workgroup to consider the adequacy, understanding, and uniformity of the access control policy and procedures regarding FSFN, including the collection of employee SSNs for access privileges. The workgroup will consider whether a FSFN-specific policy is recommended to define the Department's approach to managing access controls for current, new, and transitioning users. Also, the workgroup will make recommendations on the scope and frequency of a regular audit process to ensure consistent and appropriate practice within the established policy. Finally, the workgroup will consider the most effective mechanisms to maintain an adequate understanding of the FSFN access control policy throughout the diverse FSFN user base.

(4) Child Death Review: The Child Death Review (CDR) application is a derivative collection of information from existing data sources as a result of a reported child death in Florida related to abuse or neglect. To the extent SSNs are recorded in the CDR for individuals related to a case, those SSNs are collected from the Department's data sources with authority under Chapter 39, Florida Statutes, and Chapter 65C, Florida Administrative Code, to collect SSNs. However, the Department is currently reviewing the practice of recording SSNs within the CDR.

(5) IT Security Risk Mitigation Service: The SSN is used as the key identifier in the system to track security compliance. This system is used for everything related to security requests and provides automated reporting on security compliance such as Security Awareness Training. This system includes users who do not have other unique identifiers. A statement will be added notifying users that SSNs will be kept and stored as an encrypted key.

FINDING NO. 6: *Department controls over employee access to FLAIR and the Department's network needed improvement. Additionally, employee separation checklists used to account for the return of all State-owned property, files, records, and work product for employees separating from Department employment were not always timely or properly completed and did not always include all the required elements.*

RECOMMENDATION: *We recommend that Department management establish policies and procedures requiring periodic reviews of FLAIR access privileges to aid in the identification and resolution of any instances where excess or incompatible privileges have been granted or access privileges are no longer needed. We also recommend that Department management ensure that all employee separation checklists contain all the required information and are timely completed, and that FLAIR and network access privileges are timely deactivated upon employment termination.*

Status (per Offices of Financial Management and Information Technology Services staff): Partially Corrected

The Department will establish policies and procedures requiring periodic reviews of FLAIR access privileges and will review procedures to ensure FLAIR access privileges are timely deactivated upon employment termination.

For network access privileges, a daily report (Human Resources Tracking System-People First Daily Load Results & Terminated Employee File) is generated and sent to Department Security Officers statewide. The Security Officers use this report as confirmation or verification of termination. In addition, Office of Information Technology Services Standard Operating Procedure (SOP) S-12, §11 (*Procedure for Review of Access Levels of Current Employees and Contractors)* states that "supervisors must periodically review the access levels of current employees to ensure that current employees still require the granted access level necessary to perform their duties. The principle of least privilege must be followed. This review must be done at least once annually. The supervisor must report all access level discrepancies immediately to the Security Officer."

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.