MYFLFAMILIES.COM

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Secretary

DATE: February 27, 2017

TO: Mike Carroll
Secretary

FROM: Keith R. Parks
Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2017-004

In accordance with Section 20.055(6)(h), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2017-004, *Comprehensive Risk Assessments at Selected State Agencies,* Information Technology Operational Audit.

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

Enclosure

cc: Melinda Miguel, Chief Inspector General, Executive Office of the Governor
Kathy DuBose, Staff Director, Joint Legislative Auditing Committee

MYFLFAMILIES.COM

Mike Carroll
Secretary

DEPARTMENT OF CHILDREN AND FAMILIES

OFFICE OF INSPECTOR GENERAL
INTERNAL AUDIT

Enhancing Public Trust in Government

Keith R. Parks
Inspector General

Project #E-1516DCF-032

February 27, 2017

Six-Month Status Report

Comprehensive Risk Assessments at Selected State Agencies
Information Technology Operational Audit

PURPOSE

The purpose of this report is to provide a written response on the status of corrective actions taken six months after the Auditor General published Report No. 2017-004, ***Comprehensive Risk Assessments at Selected State Agencies,*** **Information Technology Operational Audit.**

REPORT FINDINGS, RECOMMENDATIONS, STATUS & COMMENTS

This operational audit focused on evaluating selected information technology (IT) controls applicable to the comprehensive risk assessment process at the following state agencies: Agency for Health Care Administration (AHCA), Agency for State Technology (AST), Department of Children and Families (DCF), Department of Economic Opportunity (DEO), Department of Education (DOE), and Department of Transportation (DOT).

The Office of Information Technology Services provided updated status and corrective action comments to the Auditor General's findings and recommendations. The Department was required to respond to finding numbers three and four only. 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 and staff of the aforementioned office.

FINDING NO. 3: *The risk assessment process for AHCA, DCF, DEO, DOE, and DOT did not include the classification of data and categorization of IT systems. Additionally, AHCA, DOE, and DOT did not develop risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.*

RECOMMENDATION: *To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.*

Status (per Office of Information Technology Services staff): Fully Corrected

The AST risk assessment process reviewed in this report is conducted per AST guidelines using a risk assessment Tool provided by AST. The Department complied with those guidelines. The risk assessment due March 31, 2015 was completed and submitted on March 24, 2015 by the Department's Information Security Manager (ISM). The Department followed AST guidelines and included use of the old Agency for Enterprise Information Technology (AEIT) "2015 DCF Comprehensive Risk Assessment Final.docm" template as the risk assessment tool to be completed and submitted via Secure File Transfer Protocol (SFTP). The Department has a classification tool that was available at the time, (pclaborn_1411063698_Data Collection Request DCF 08.06.14 v2 compiled.xlsx) but this was not included in the AEIT template that the Department received from AST. In addition, AST did not request it as part of this three-year exercise. The Department, however, provided this tool to the AST security team in August 2014 and AST had a copy.

The AST controlled template (the old AEIT template) did not include space for categorization of DCF systems, nor did it request it. The Department submitted it in a separate spreadsheet. The Department had categorized its systems according to Federal Information Processing Standards (FIPS) 199.

FINDING NO. 4: *Selected IT security controls for AHCA, DCF, DEO, DOE, and DOT need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.*

RECOMMENDATION: *To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.*

Status (per Office of Information Technology Services staff): Fully Corrected

On December 16, 2016, the Department completed an AST risk assessment per Specific Appropriation 1961B of the 2016-2017 General Appropriations Act (Proviso), which tasked AST with establishing a risk assessment methodology and procurement approach for 16 state agencies to use to procure security risk assessment services. The Department was one of the 16 agencies selected to participate in the risk assessment. The Department completed and submitted the new risk assessment tool provided by AST (FCS_RiskAssessmentTool_V1.0.xlsx)) on the January 10, 2017 due date and confirmed receipt with AST via email. The AST risk assessment was conducted against the National Institute of Standards and Technology (NIST) 800-53 Revision 4 controls specified by AST, as their Cybersecurity Framework for Risk Assessment (http://www.ast.myflorida.com/ciso_cybersecurity-framework.asp) and based upon the new required security controls per the 2016 Florida Administrative Code (FAC) §74-2. This was a noted improvement upon the AEIT template, as the old AEIT template used by AEIT was based on old retired FAC §71A-1 required security controls.

This follow-up audit was conducted as required by Florida Statutes 20.055(6)(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.