



**State of Florida
Department of Children and Families**

Ron DeSantis
Governor

Chad Poppell
Secretary

DATE: April 12, 2019

TO: Chad Poppell
Secretary

FROM: Keith R. Parks
Inspector General

SUBJECT: Six-Month Status Report for Auditor General Report No. 2019-022

In accordance with Section 20.055(6)(h), Florida Statutes, enclosed is our six-month status report on Auditor General Report No. 2019-022, *Department of Children and Families, Florida Online Recipient Integrated Data Access (FLORIDA) System*.

The Office of Information Technology Services and Office of Economic Self-Sufficiency provided updates, which indicate that the recommendations to Findings #1 and #2 have been fully implemented. Recommendations to Findings #3 through #7 have been partially implemented.

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
Patricia Babcock, Deputy Secretary
David Mica, Chief of Staff
Julie Madden, Chief Information Officer
Taylor Hatch, Assistant Secretary for Economic Self-Sufficiency

KP/SM/ej

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Work in Partnership with Local Communities to Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery and Resiliency

OIG – Internal Audit
Corrective Action Status Report
Florida Online Recipient Integrated Data
Access (FLORIDA) System
Report No. 2019-022, Issued September 12, 2018
As of April 5, 2019

Findings	Recommendation	Auditee Response	Corrective Action Status
<p>Finding 1</p> <p>The Department did not timely review and process numerous data exchange responses, increasing the risk that benefits may not be paid timely or accurately. Similar findings were noted in prior audits, most recently in report No. 2017-009.</p>	<p>Recommendation 1. a.</p> <p>We again recommend that Department management improve controls to ensure that data exchange responses are reviewed and processed within the time frames established by Department policy.</p> <p>Recommendation 1. b.</p> <p>We also recommend that the Department retain all data exchange responses necessary to demonstrate compliance with applicable Federal requirements.</p>	<p>The Department concurs with this finding. The Department has improved controls through the implementation of the Data Exchange (DE) system controls and automation enhancement on September 26, 2016, which prevents eligibility staff from authorizing benefits prior to processing un-reviewed DEs. Since implementation, staff have processed 11,191,206 DEs and in turn reduced the backlog to 625,232 overdue DEs as of August 14, 2018. Overdue DEs have been reduced from 1.6 million on April 10, 2015 (Florida Auditor General Report No. 2016-007) to 1 million on May 18, 2016 (Florida Auditor General Report No. 2017-009) to 650,131 on November 29, 2017 (current finding), representing a decrease of 59%. As of August 14, 2018, the number of overdue DEs is 625,232, which is an overall decrease of 61% from April 2015 to August 2018.</p> <p>Effective January 9, 2017, the Department retains all data exchange responses necessary to demonstrate compliance with applicable Federal requirements.</p> <p>The Department has made significant gains in its effort to reduce overdue DEs and ensure DEs are reviewed and processed within the established timeframes. The Department will continue its efforts to make further improvements.</p>	<p>Fully Implemented</p> <p>All activities implemented as of January 2017.</p>

**OIG – Internal Audit
 Corrective Action Status Report
 Florida Online Recipient Integrated Data
 Access (FLORIDA) System
 Report No. 2019-022, Issued September 12, 2018
 As of April 5, 2019**

<p>Finding 2 The Department's change management controls need improvement to ensure that FLORIDA System calculation and reason code table changes follow the Department's established change management processes and changes are properly authorized, tested, and approved for implementation.</p>	<p>Recommendation 2.a. We recommend that Department management ensure that all application and data changes implemented into the production environment, including FLORIDA System calculation and reason code table changes, follow the Department's established change management processes to ensure that the changes are properly authorized, tested, and approved for implementation.</p> <p>Recommendation 2.b. Additionally, we recommend that Department management revise the change management process to include the reconciliation of changes implemented into production to the authorized changes documented in ClearQuest.</p> <p>Recommendation 2.c. We also recommend that the change management process for policy changes be enhanced to include review and approval by the ESS Office of Program Policy prior to implementation of the changes.</p>	<p>Currently, ClearQuest does not support the ability for the ESS Program Office to sign-off officially on the table change request. Therefore, a process has been developed by which the ESS Program Office sends a table change request form to the Office of Information Technology Services (OITS), who in turn creates the change request. Once the table changes have been completed, OITS verifies and then sends them to the ESS Program Office for final verification in acceptance before moving them to production. The ESS Program Office also has final review of the production change as well.</p> <p>The Department agrees that – for the time period of the OAG FLORIDA Audit, 10/1/2016 – 1/1/2018 – there were examples of requested changes to FLORIDA System calculation and code tables that were not documented and tracked in the Department's change management tool (ClearQuest). The original intent of relaxing requirements for tracking changes to these tables was to provide more responsive service to the ACCESS Program Office by allowing requests to be made via email. However, it was determined that email was an ineffective tool for tracking calculation and code table changes. The Department reverted back to requiring all changes to be tracked and managed in ClearQuest starting March 2018. The Department currently meets the recommendation for this finding.</p>	<p>Fully Implemented The process was implemented May 2018.</p> <p>The department agrees that calculation and code tables were not documented and tracked in the Department's change management tool (ClearQuest). The original intent of relaxing requirements for tracking changes to those tables was to provide more responsive service to the ESS Program Office by allowing requests to be made via e-mail. However, it was determined that e-mail was an ineffective tool for tracking calculation and code table changes. The department reverted to requiring all changes to be tracked and managed in ClearQuest starting March 2018. As of August 22, 2018, the department meets the recommendation for this finding.</p>
---	--	--	---

OIG – Internal Audit
Corrective Action Status Report
Florida Online Recipient Integrated Data
Access (FLORIDA) System
Report No. 2019-022, Issued September 12, 2018
As of April 5, 2019

Findings	Recommendation	Auditee Response	Corrective Action Status
<p>Finding 3 Certain Department change management procedures contained outdated information and the Department had not established some necessary change management procedures.</p>	<p>Recommendation 3. We recommend that Department management continue efforts to ensure that applicable change management procedures are documented and kept up-to-date.</p>	<p>The Department agrees with this finding. The OITS will work with the ACCESS Program Office to establish written procedures for documenting the receipt of changes for Federal program requirements and the tracking of those changes affecting FLORIDA System table changes. Projected resolution date for this finding is July 1, 2019. month.</p>	<p>Partially Implemented Ongoing efforts are in place to work with the ESS program office to develop a consistent, documented procedure for the Change Management process.</p>
<p>Finding 4 Documentation supporting authorization of access privileges to the FLORIDA System and the Automated Community Connection to Economic Self-Sufficiency (ACCESS) Management System (AMS) for some employees was missing, incomplete, or incorrect. Similar findings were noted in prior audits, most recently in report No. 2017-009.</p>	<p>Recommendation 4. We again recommend that Department management improve controls to ensure that access authorization forms are retained, complete, and commensurate with management's direction and that access privileges are only granted as indicated on the access authorization forms.</p>	<p>The Department agrees that there have been instances discovered in which ACCESS Security Forms are incomplete or missing. The OITS will continue to work with Headquarters and Regional Security Officers to reinforce compliance with security form storage and archival requirements. The Department is currently evaluating the feasibility of automating ACCESS Security Forms in order to more effectively access, track and update systems access authorizations. Projected resolution date for this finding is July 1, 2019.</p>	<p>Partially Implemented Effective January 11, 2019, the Department implemented a pilot of the Security Audit System. This system incorporates data from multiple systems to determine users who need updates to their system access. A message will be sent to the local security officer to determine the change needed.</p>

**OIG – Internal Audit
 Corrective Action Status Report
 Florida Online Recipient Integrated Data
 Access (FLORIDA) System
 Report No. 2019-022, Issued September 12, 2018
 As of April 5, 2019**

Findings	Recommendation	Auditee Response	Corrective Action Status
<p>Finding 5 The Department did not conduct comprehensive periodic reviews of the appropriateness of user access privileges granted to the FLORIDA System and the AMS. Similar findings were noted in prior audits, most recently in report No. 2017-009.</p>	<p>Recommendation 5. We again recommend that Department management conduct a comprehensive periodic review of access privileges for the FLORIDA System and the AMS and establish procedures to ensure that the reviews are performed annually as required by SOP S-12.</p>	<p>The Department agrees that periodic reviews of user access privileges should be required and enforced and, to that end, has undertaken the development of an automated system (Security Audit System) that will allow managers and supervisors statewide the ability to review and approve access privileges. This system is scheduled to be deployed as a pilot in the DCF Suncoast Region by September 2018, and, pending the outcome of the pilot program will be deployed for statewide use in FY 2018-2019.</p>	<p>Partially Implemented Effective January 11, 2019, the Department implemented a pilot of the Security Audit System. This system incorporates data from multiple systems to determine users who need updates to their system access. A message will be sent to the local security officer to determine the change needed.</p>
<p>Finding 6 Some Department users had inappropriate access privileges to FLORIDA System resources, increasing the risk that unauthorized modification, loss, or disclosure of FLORIDA System IT resources may occur.</p>	<p>Recommendation 6. We recommend that Department management limit user access privileges to the FLORIDA System to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.</p>	<p>The Department agrees with this finding. The assignment of access privileges was designed to allow flexibility in user's roles so that workload impact on units could be mitigated by as needed assignment of roles. The Department will review access privileges of users and limit access privileges where possible to ensure compliance with least privilege principles. This will include limiting an HQ security officer's profile to modify table changes to only to specific individuals who will be performing this function. Projected resolution date for this finding is July 1, 2019.</p>	<p>Partially Implemented A new user profile/role needs to be created prohibit users with a security coordinator role from the ability to modify reference tables. Table modifications should be limited to certain key individuals. The ESS program office is reviewing whether a new role should be created and, if so, which individuals should be granted access to modify tables. In addition, the Security Audit System will also rectify this issue in the future.</p>

OIG – Internal Audit
Corrective Action Status Report
Florida Online Recipient Integrated Data
Access (FLORIDA) System
Report No. 2019-022, Issued September 12, 2018
As of April 5, 2019

Findings	Recommendation	Auditee Response	Corrective Action Status
<p>Finding 7 Certain security controls related to the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access for the FLORIDA System and the AMS, and related IT resources, continue to need improvement to ensure the confidentiality, integrity, and availability of the FLORIDA System and the AMS data and related IT resources.</p>	<p>Recommendation 7. We recommend that Department management improve security controls related to the protection of confidential and exempt data, logging and monitoring, user authentication, and logical access to ensure the confidentiality, integrity, and availability of FLORIDA System and AMS data and related IT resources.</p>	<p>The Department agrees with this finding. The Department received funding in FY 2017-2018 and FY 2018 – 2019 to implement tools and programs to comply with the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standard for Exchanges (MARS-E) 2.0 Security and Privacy Controls based on the NIST 800-53 Rev 4 standards. In July 2018, the Department implemented a Security Information and Event Monitoring (SIEM) tool that allows wide ranging auditing, reporting and data analytics functions for logging and monitoring of systems activities, including user access to applications, networks and IT resources. In FY 2018-2019 the Department will greatly expand its MARS-E 2.0 compliance efforts by implementing a variety of security tools and programs as well as new and updated policies and procedures governing security and privacy controls.</p>	<p>Partially Implemented On January 7, 2019, the initial kick-off meeting occurred with the Infrastructure team to discuss the implementation of Network Access Control tools, Wireless Intrusion Detection Systems, into the current DCF network. The Department has not set an implementation date yet. A SIEM tool has been incorporated into the DCF/ACCESS process. Other security control systems/processes currently pending are: Data Governance/Classification program, Data Loss Prevention program, and Role-based Information Security Training Program. The anticipated Implementation date of these processes are June 30, 2019.</p>