JLAC received 7.14.25

Florida Department of Revenue
Office of Inspector General

Jim Zingale
Executive Director

5050 West Tennessee Street, Tallahassee, FL 32399

floridarevenue.com

July 11, 2025

MEMORANDUM

TO: Jim Zingale, Executive Director

FROM: Angie Welch, Inspector General

SUBJECT: Six-Month Update on Auditor General Report Number 2025-162, State of Florida - Compliance and Internal Controls Over Financial Reporting and Federal Awards

As required by *section* 20.055(6)(h), Florida Statutes (F.S.), attached is the Department's six-month status update for corrective actions taken in response to Auditor General Report Number 2025-162, State of Florida - Compliance and Internal Controls Over Financial Reporting and Federal Awards.

The Information Services Program (ISP) in coordination with the General Tax Program (GTA) and the Child Support Program provided updates on actions taken to correct the following findings:

Finding No. 2024-014 (Confidential finding):
Effective information technology (IT) security controls include mechanisms such as personal passwords for authenticating a user's identity to a system. Controls protecting the confidentiality of an authenticator type, such as passwords, are necessary to ensure that unauthorized individuals do not inappropriately gain access to data and related IT resources. Department of Management Services (DMS) rules require the use of multi-factor authentication (MFA) for access to networks or applications that have a risk categorization of moderate or high or that contains exempt (sensitive), or confidential and exempt, information, and for access to privileged (administrative) accounts.

As part of our audit, we evaluated the adequacy of authentication controls for the System for Unified Taxation (SUNTAX). Our inquiries of Florida Department of Revenue (FDOR) management disclosed that certain users accessed SUNTAX using a single sign-on process through the FDOR's network, and other users accessed SUNTAX directly by a separate sign-on process. We noted that, although these environments require enhanced security, including MFA, the FDOR did not require MFA for all users that accessed SUNTAX directly by a separate sign-on process, contrary to DMS rules. According to FDOR management, due to a mandatory SAP software update to SUNTAX

that limits the ability to implement changes, the Department accepted the risk of delaying implementation of a control at the application layer for the systems.

Appropriate user authentication controls, including MFA for all SUNTAX users, are necessary to decrease the risk that unauthorized individuals may gain access to SUNTAX and compromise the confidentiality, integrity, and availability of SUNTAX data and related IT resources.

Recommendation: We recommend that FDOR management improve user authentication controls by implementing MFA for all SUNTAX users.

Status: Partially Completed - The anticipated completion date is December 31, 2025 at the network level and December 31, 2028 at the application level. The long-term goal of adding MFA to external SUNTAX access at the DOR Network perimeter is scheduled for December 31, 2025. The long-term goal to add MFA at the application layer remains contingent on the Department's SAP software updated. Michele Baxley-Branch, Data Processing Services Process Manager, provided the response on July 7, 2025.

Finding No. 2024-036 (Confidential finding):
Effective information technology (IT) security controls include mechanisms such as personal passwords for authenticating a user's identity to a system. Controls protecting the confidentiality of an authenticator type, such as passwords, are necessary to ensure that unauthorized individuals do not inappropriately gain access to data and related IT resources. Department of Management Services (DMS) rules require the use of MFA for access to networks or applications that have a risk categorization of moderate or high or that contain exempt (sensitive), or confidential and exempt, information, and for access to privileged (administrative) accounts.

As part of our audit, we evaluated the adequacy of authentication controls for the Child Support Enforcement Automated Management System (CAMS). Our inquiries of Florida Department of Revenue (FDOR) management disclosed that certain users accessed CAMS using a single sign-on process through the FDOR's network, and other users accessed CAMS directly by a separate sign-on process. We noted that, although these environments required enhanced security, including MFA, the FDOR did not require MFA for all users that accessed CAMS directly by a separate sign-on process, contrary to DMS rules. According to FDOR management, due to a mandatory SAP software update to CAMS that limits the ability to implement changes, the Department accepted the risk of delaying implementation of a control at the application layer for these systems.

Appropriate user authentication controls, including MFA for all CAMS users, are necessary to decrease the risk that unauthorized individuals may gain access to CAMS and compromise the confidentiality, integrity, and availability of CAMS data and related IT resources.

Recommendation: We recommend that FDOR management improve user authentication controls by implementing MFA for all CAMS users.

Status: Partially Completed - We will be implementing MFA to the application layer only. The anticipated completion date is June 30, 2028. Kevin Wiggins, Information Security Manager, provided the response on July 7, 2025.

If you have any questions, please contact me at (850) 617-8152, or Stacey Emminger, Audit Director, at (850) 717-6710.

AW/

cc:
Clark Rogers, Deputy Executive Director/Chief of Staff
Jimmie Harrell, ISP Program Director
Maria Johnson, GTA Program Director
Ann Coffin, Child Support Program Director
Joint Legislative Auditing Committee