STATE OF FLORIDA

Office of the Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001

www.flgov.com
850-717-9418

RON DESANTIS
GOVERNOR

January 14, 2025

The Honorable Ron DeSantis
Governor of the State of Florida
The Capitol, PL 05
Tallahassee, FL 32399

Dear Governor DeSantis:

On July 17, 2024, the Auditor General released Report Number 2025-001, *State Budgetary Process and Information Technology Controls.*

In accordance with Section 20.055, Florida Statutes, and applicable auditing standards, the Office of the Chief Inspector General has established a system to monitor the disposition of results communicated to management to ensure corrective actions related to findings and recommendations have been effectively implemented.

After six months, the results of our monitoring disclosed that corrective action has been implemented for three of the findings, and management has accepted the risk on one finding. All findings have been addressed, and no further monitoring will be performed. Pursuant to Section 20.055(6)(h), Florida Statutes, a copy of this response will be filed with the Joint Legislative Auditing Committee.

I am available at your convenience to discuss this matter further.

Respectfully,

Melinda M. Miguel
Chief Inspector General

Enclosure

cc/enc: James Uthmeier, Chief of Staff
           Brandi Gunder, Deputy Budget Director
           Daniel Pardo, Deputy Director of Policy
           Dawn Hanson, Director of Administration
           Alan T. Cash, Chief Information Officer
           Michael Jones, Office of Policy and Budget, System Development and Design

Executive Office of the Governor
Office of the Chief Inspector General

CORRECTIVE ACTION PLAN

Report Title
State Budgetary Processes and Information
Technology Controls – Operational Audit

Report Issued By
Florida Auditor General

Report Number
No. 2025-001

OCIG Contact Person/Phone
Steven Henry / (850) 717-9255

Original Report Date
July 17, 2024

Due to Office of Chief Inspector General
Friday, January 3, 2025

The Executive Office of the Governor, Office of the Chief Inspector General (OCIG) coordinates all responses to internal and external audits, reviews, and other assessments that require a written response. This document serves to provide management an opportunity to formally respond with your initial or updated corrective actions in relation to the report listed above.

Please complete the section labeled "Management's Current Response" for each of the findings and recommendations listed below. If this is an initial Corrective Action Plan (CAP), the section labeled "Management's Previous Response" will be shown as N/A. If this is a follow-up CAP, management's most recent substantive response will be provided for informational purposes.

Also, follow-up CAPs may contain what appear to be "missing" findings (i.e. non-sequential finding numbers). This will indicate the "missing" findings were previously reported to be fully corrected and thus no further response is needed.

<u>Please be aware, statutory requirements often apply to the timing of your response to reports issued by an audit entity. To ensure compliance with these statutory requirements, it is critically important this document be completed and returned no later than the date listed above.</u>

For any corrective actions you are reporting as "Completed" in this CAP, please provide supporting documentation, if possible, when returning this document. Please label any supporting documentation with the finding number the documentation supports. All corrective actions reported as being completed in this CAP will be verified by OCIG staff.

If you have questions or need additional information, please contact the OCIG representative listed above.

Corrective Action Plan in response to:
No. 2021-059: Information Technology Controls Prior Audit Follow-Up

---

Finding 1: **User Access to the OPB Network, LAS/PBS, and BAPS.**

EOG controls over access to the Office of Policy and Budget (OPB) network, the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem (LAS/PBS), and the Budget Amendment Processing System (BAPS) need improvement.

Recommendation: We recommend that EOG management conduct reviews of the appropriateness of OPB network, LAS/PBS, and BAPS user access privileges at least quarterly and ensure that OPB network, LAS/PBS, and BAPS user access privileges are immediately removed upon a user's separation from EOG employment or when the access is no longer required.

Does Management Concur with the <u>Finding</u>? ☒Yes ☐ No (this <u>DOES NOT</u> include the recommendation)
Explain a "No" answer:

Management's Current Response

Current Status: *Completed
* Provide supporting documentation for "Completed" corrective actions (where possible)

Description of Corrective Action(s) or Explanation of No Action:
SDD has increased the frequency of the security reviews. As this is a continuing effort there is no true completion date.

Projected Completion Date: 1/6/2025
Contact Person/Phone: Michael Jones (850) 717-9451

Management's Previous Response

Date of Response: July 16, 2024

Description of Corrective Action(s): Systems Design and Development will institute more frequent (quarterly) reviews of access privileges for OPB and SDD users. This will ensure that users no longer with OPB/SDD do not have access to sensitive systems. SDD will also document when OPB requests that user accounts remain active beyond the employee termination date and when the password for the account was changed.

Projected Completion Date: Not Provided
Contact Person/Phone: Michael Jones, (850) 717-9451

Finding 2: **Security Controls – User Authentication.**

Certain security controls related to OPB network, LAS/PBS, and BAPS user authentication need improvement to ensure the confidentiality, integrity, and availability of EOG data and IT resources.

Recommendation: We recommend that EOG management enhance certain security controls related to OPB network, LAS/PBS, and BAPS user authentication to ensure the confidentiality, integrity, and availability of EOG data and related IT resources.

Does Management Concur with the <u>Finding</u>? ☒Yes ☐ No (this <u>DOES NOT</u> include the recommendation)
Explain a "No" answer:

Corrective Action Plan in response to:
No. 2021-059: Information Technology Controls Prior Audit Follow-Up

Management's Current Response

Current Status: *Completed
Provide supporting documentation for "Completed" corrective actions (where possible)

Description of Corrective Action(s) or Explanation of No Action:
SDD has implemented Multi-Factor Authentication in several aspects of the environment.

Projected Completion Date: 1/6/2025
Contact Person/Phone: Michael Jones, (850) 717-9451

Management's Previous Response

Date of Response: July 16, 2024

Description of Corrective Action(s): SDD will enhance security controls in the recommended areas to provide increased protection to the LAS/PBS environment.

Projected Completion Date: Not Provided
Contact Person/Phone: Michael Jones, (850) 717-9451

Finding 3: **Change Management Controls.**

EOG records did not always evidence that BAPS programming change duties were appropriately separated. Similar findings have been noted in prior audit reports, most recently in our report No. 2021-059.

Recommendation: We again recommend that EOG management enhance change management controls to ensure that duties for BAPS programming changes are properly separated and the identity of each responsible individual in the change management process is documented.

Does Management Concur with the Finding? ☒Yes ☐ No (this DOES NOT include the recommendation)
Explain a "No" answer:

Management's Current Response

Current Status: *Completed
Provide supporting documentation for "Completed" corrective actions (where possible)

Description of Corrective Action(s) or Explanation of No Action:
SDD continues to perform the measures documented in the previous response

Projected Completion Date: 1/6/2025
Contact Person/Phone: Michael Jones (850) 717-9451

Management's Previous Response

Date of Response: July 16, 2024

Corrective Action Plan in response to:
No. 2021-059: Information Technology Controls Prior Audit Follow-Up

Description of Corrective Action(s): SDD recognizes the importance of proper change management and the separation of responsibilities. However, as previously noted, the limited number of staff in the programming areas prevents the ability to enforce these standards. SDD will ensure that appropriate information will be entered into Azure DevOps to track programs changes and the staff responsible for making those changes.

Projected Completion Date: Not Provided
Contact Person/Phone: Michael Jones, (850) 717-9451

Finding 4: **Mobile Device Security Controls.**

Certain security controls over OPB employee mobile device utilization continue to need improvement to ensure the confidentiality, integrity, and availability of EOG data and IT resources.

Recommendation: We again recommend that EOG management enhance certain security controls related to OPB employee use of mobile devices to ensure the confidentiality, integrity, and availability of EOG data and IT resources.

Does Management Concur with the Finding? ☒Yes ☐ No (this DOES NOT include the recommendation)
Explain a "No" answer:

Management's Current Response

Current Status: *Completed
* Provide supporting documentation for "Completed" corrective actions (where possible)

Description of Corrective Action(s) or Explanation of No Action:
SDD understands and accepts the risks associated with the current mobile device policy. No change in policy will be made at this time.

Projected Completion Date: **1/6/2025**
Contact Person/Phone: Michael Jones (850) 717-9451

Management's Previous Response

Date of Response: July 16, 2024

Description of Corrective Action(s): SDD understands and accepts the risks associated with the current mobile device policy. No change in policy will be made at this time.

Projected Completion Date: Not Provided
Contact Person/Phone: Michael Jones, (850) 717-9451