STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2025-001
July 2024

EXECUTIVE OFFICE OF THE GOVERNOR

State Budgetary Processes and Information Technology Controls

Sherrill F. Norman, CPA
Auditor General

Executive Office of the Governor

Pursuant to Section 14.201, Florida Statutes, the Governor is the head of the Executive Office of the Governor. The Honorable Ron DeSantis served as Governor during the period of our audit.

The team leader was Thomas E. Drawbaugh, CPA, and the audit was supervised by Karen W. Van Amburg, CPA.

Please address inquiries regarding this report to Karen W. Van Amburg, CPA, Audit Manager, by e-mail at karenvanamburg@aud.state.fl.us or by telephone at (850) 412-2766.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

EXECUTIVE OFFICE OF THE GOVERNOR

State Budgetary Processes and Information Technology Controls

SUMMARY

This operational audit of the Executive Office of the Governor (EOG) focused on State budgetary processes and information technology (IT) controls. The audit also included a follow-up on the findings noted in our report No. 2021-059. Our audit disclosed the following:

Finding 1: 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.

Finding 2: 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.

Finding 3: 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.

Finding 4: 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.

BACKGROUND

The State Constitution[1] vests the supreme executive power of the State in the Governor and designates the Governor as the chief administrative officer of the State, responsible for State planning and budgeting. State law[2] establishes the Governor as the head of the Executive Office of the Governor (EOG) and the Governor utilizes various offices within the EOG to promote the efficient operation of State Government. For the 2023-24 fiscal year, the Legislature appropriated approximately $53 million to the EOG and authorized 284 positions.[3]

FINDINGS AND RECOMMENDATIONS

State law[4] requires State agencies to establish cybersecurity controls to ensure the security of agency data, information, and information technology (IT) resources. Additionally, Department of Management Services (DMS) rules[5] establish minimum cybersecurity standards for ensuring the confidentiality, integrity, and availability of State agency data, information, and IT resources.

[1] Article IV, Section 1(a) of the State Constitution.

[2] Section 14.201, Florida Statutes.

[3] Chapter 2023-239, Laws of Florida. Figures do not include amounts appropriated to and positions authorized for the Division of Emergency Management within the EOG.

[4] Section 282.318(4), Florida Statutes.

[5] DMS Rules Chapter 60GG-2, Florida Administrative Code.

The Executive Office of the Governor (EOG), Office of Information Systems (OIS), provided IT resource support and information security policies and procedures for all EOG programs, activities, and functions, except the Office of Policy and Budget (OPB) within the EOG. The OPB, Systems Design and Development Unit (SDD), was responsible for administering a separate network that included OPB applications and systems, including the OPB e-mail system. Our audit included an evaluation of selected controls related to the OPB network, the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem (LAS/PBS), and the Budget Amendment Processing System (BAPS).

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

DMS rules[6] require State agencies to review access privileges periodically based on system categorization or assessed risk and ensure that IT access privileges are removed when access to an IT resource is no longer required. Periodic (e.g., quarterly) reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. Prompt action to deactivate user access privileges upon employment separation or when no longer required is necessary to help prevent misuse of the access privileges.

As part of our audit, we inquired of SDD management and compared People First[7] records to OPB network, LAS/PBS, and BAPS disablement date records for the employees who separated from EOG employment during the period December 2020 through January 2022. Our audit procedures found that:

- User access to the OPB network, LAS/PBS, and BAPS was only reviewed annually.
- OPB network access privileges for 2 of the 30 employees who separated from EOG employment remained active as of January 2022, although 99 and 274 days had elapsed since the employees separated from EOG employment. According to SDD management, the access privileges for the 2 employees were not timely removed due to oversights. Additionally, OPB network access privileges for 6 other employees remained active 1 to 53 days (an average of 16 days) after the employees' separation dates. In response to our audit inquiry, SDD management indicated that the OPB had not timely requested that 5 of the employees' network access privileges be removed, and access privileges for the sixth employee had been left active for 10 days to ensure that the employee's programming code had been successfully migrated to production. A similar finding has been noted in previous audits of the EOG, most recently in our report No. 2021-059 (Finding 3).
- User access privileges to the LAS/PBS and BAPS were not always timely removed. Specifically:
    - Access privileges for 1 of the 20 employees with access privileges to the LAS/PBS who separated from EOG employment remained active as of May 2022, due to an oversight, although 209 days had elapsed since the employee separated from EOG employment. In addition, LAS/PBS access privileges for 6 other employees were not removed until 3 to 242 days (an average of 100 days) after the employees separated from EOG employment.
    - Access privileges for 1 of the 22 employees with access privileges to BAPS who separated from EOG employment remained active as of May 2022, although 156 days had elapsed since the employee separated from EOG employment. Also, access privileges for 18 other

[6] DMS Rule 60GG-2.003(1)(a)6. and 8., Florida Administrative Code.

[7] People First is the State's human resource information system. People First maintains employee information, including hire and separation dates.

employees had been removed 1 to 157 days (an average of 42 days) after the employees separated from EOG employment.

In response to our audit inquiry, SDD management indicated that in some instances user access privileges were kept active after an employee's separation date to provide data needed by replacement staff and that passwords were typically changed to prevent subsequent access by former employees. Notwithstanding, as SDD management did not retain documentation evidencing the dates the former employees' passwords were changed, management was unable to show that the passwords were timely changed upon separation from EOG employment.

Reviews of OPB network, LAS/PBS, and BAPS user access privileges conducted at least quarterly would provide EOG management additional assurance that user access privileges are authorized and remain appropriate. Additionally, as unauthorized access can occur at any time, promptly disabling user OPB network, LAS/PBS, and BAPS access privileges upon employment separation or when no longer required reduces the risk that the access privileges may be misused by a former employee or others.

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.

Finding 2: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to OPB network, LAS/PBS, and BAPS user authentication need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising EOG data and IT resources. However, we have notified appropriate EOG management of the specific issues.

Without appropriate security controls related to OPB network, LAS/PBS, and BAPS user authentication, the risk is increased that the confidentiality, integrity, and availability of EOG data and IT resources may be compromised.

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.

Finding 3: Change Management Controls

To promote effective change management over IT resources, DMS rules[8] require State agencies to establish a change control process to manage upgrades and modifications to existing IT resources. Effective change management controls ensure that all changes (program or functionality changes) follow a change management process that provides for an appropriate separation of duties and ensures that changes are appropriately authorized, reviewed and tested, approved, and moved to production. Additionally, agency controls should clearly document and track the change management process from initial authorization of the change to final approval.

[8] DMS Rule 60GG-2.003(5)(c), Florida Administrative Code.

The SDD utilized Azure DevOps Server to track changes to BAPS and to document, for each change, the identity of the requestor, programmer, tester, and individual responsible for implementing the programming change into the production environment. As part of our audit, we inquired of SDD management and examined Azure DevOps Server records for 18 of the 200 BAPS change requests made during the period November 2020 through January 2022 and found that OPB-SDD records did not always document the identity of the responsible individual or demonstrate appropriate separation of duties. Specifically:

- 6 of 14 applicable BAPS program changes did not evidence the individual responsible for implementing the change into production.
- 8 of 14 applicable BAPS program changes indicated that the individual responsible for making the change was the same individual responsible for implementing the change into the production environment.

In response to our audit inquiry, SDD management indicated that a limited number of personnel prevented the separation of duties; however, the SDD was using Azure DevOps Server with version control that provided notifications if changes were made to underlying program code as part of a build. Notwithstanding, the proper separation and documentation of change management duties and actions strengthens the effectiveness of SDD change management controls by ensuring that changes are appropriately made and tracked from initiation to deployment. Similar findings have been noted in prior audits of the EOG, most recently in our report No. 2021-059 (Finding 4).

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.

Finding 4: Mobile Device Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to OPB employee mobile device[9] utilization need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising EOG data and IT resources. However, we have notified appropriate EOG management of the specific issues.

Without appropriate security controls related to the use of mobile devices by OPB employees, the risk is increased that the confidentiality, integrity, and availability of EOG data and IT resources may be compromised. A similar finding has been noted in previous reports, most recently in our report No. 2021-059 (Finding 5).

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.

[9] Mobile devices are portable devices, such as laptop computers, smartphones, and tablets, that allow storage and transmittal of entity data.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the EOG had taken corrective actions for the findings included in our report No. 2021-059.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from February 2022 through September 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This operational audit of the Executive Office of the Governor (EOG) focused on State budgetary processes. For those areas, the objectives of the audit were to:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering responsibilities in accordance with applicable laws, administrative rules, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed into operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, the reliability of records and reports, and the safeguarding of assets, and identify weaknesses in those internal controls.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

Our audit also included steps to determine whether management had corrected, or was in the process of correcting, all deficiencies noted in our report No. 2021-059.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, deficiencies in internal controls significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; identifying and evaluating internal

controls significant to our audit objectives; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of transactions and records. Unless otherwise indicated in this report, these transactions and records were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed applicable laws, rules, EOG policies and procedures, and other guidelines, and interviewed EOG personnel to obtain an understanding of Office of Policy and Budget (OPB) processes and responsibilities.
- Inquired of EOG management regarding whether the EOG made any expenditures or entered into any contracts under the authority granted by an applicable state of emergency during the period July 1, 2021, through February 17, 2022.
- Obtained an understanding of selected OPB information technology (IT) controls, assessed the risks related to those controls, evaluated whether selected general and application IT controls for the OPB network, Legislative Appropriations Subsystem/Planning and Budgeting Subsystem (LAS/PBS), and Budget Amendment Processing System (BAPS) were in place, and tested the effectiveness of the selected controls.
- Inquired of OPB personnel and selected and examined OPB records for the 20 employees with LAS/PBS access and 22 employees with BAPS access who separated from EOG employment during the period December 2020 through January 2022 to determine whether user access privileges to the LAS/PBS and BAPS were timely disabled upon an employee's separation from EOG employment.
- Examined the Master Fiscal Year Legislation report, Contingent Discretionary Fund report, and budget release memoranda for the 2020-21 fiscal year, and the Reorganizations report, Governor's Budget Recommended Reorganizations report, and the Schedule of Trust Fund Revenues and Unreserved Fund Balance for the 2021-22 fiscal year to determine whether the reports, memoranda, and schedule were accurate, complete, timely prepared, and adequately supported.
- From the population of 239 fixed capital outlay (FCO) appropriations totaling $12,749,529,282 and available to State agencies during the period July 2020 through January 2022, examined OPB records for 33 selected FCO appropriations totaling $5,428,240,290 to determine whether the OPB complied with applicable laws, rules, and guidelines when reviewing State agency FCO appropriations and associated requests for appropriations releases.
- Identified 50 new Federal grants on the State's 2020-21 fiscal year Schedule of Expenditures of Federal Awards (SEFA) with expenditures totaling $2,895,491,206 and examined available documentation of approvals for 6 selected grants with expenditures totaling $2,622,096,800 to determine whether EOG procedures ensured that State agency requests for Federal funds were approved by the EOG and that the grants were included in the Federal Grants Tracking System.

- From the population of 79 LAS/PBS users as of May 2022 and 78 BAPS users as of June 2022, examined OPB user access records for 13 selected LAS/PBS users and 20 selected BAPS users to determine whether user access to the systems was appropriately authorized.
- Examined OPB records related to the 2021-22 fiscal year recommended budget appropriations report submitted to the Legislature to determine whether the budget recommendations were prepared accurately, timely, and in accordance with applicable provisions of Chapters 215 and 216, Florida Statutes, and EOG policies and procedures.
- From the population of 31 legislative budget requests (LBRs) and 32 long-range program plans (LRPPs) submitted to the EOG by 30 State agencies for the 2021-22 fiscal year, examined OPB records related to 10 selected LBRs and 10 selected LRPPs submitted by 10 State agencies to determine whether the OPB took appropriate actions to ensure that State agencies timely submitted accurate LBR and LRPP documents that included all required information.
- From the population of 1,657 budget amendments submitted through BAPS for the 2021-22 fiscal year, examined OPB records for 25 selected budget amendments to determine whether OPB procedures ensured that the amendments were reviewed for compliance with applicable laws and OPB procedures and approved, as appropriate.
- Evaluated EOG actions to correct the findings noted in our report No. 2021-059. Specifically, we:
    - Inquired of EOG personnel and reviewed EOG organization charts and policies and procedures to determine whether the EOG designated an Information Security Manager (ISM) to the Department of Management Services (DMS) by January 1, 2021 and 2022, and whether the ISM reported directly to the Governor for information security duty purposes, in accordance with Section 282.318(4)(a), Florida Statutes.
    - Inquired of EOG personnel, reviewed EOG policies and procedures, and examined EOG records for the 56 employees who began employment with the EOG during the period January 2021 through January 2022 and for 5 other selected EOG employees and 23 other selected Systems Design and Development Unit employees who were not newly hired to determine whether EOG policies and procedures required all personnel to timely complete security awareness training in accordance with DMS information security rules, whether new employees completed information security awareness training within 30 days of hire, and whether employees completed annual information security awareness training.
    - Inquired of EOG personnel and selected and examined OPB records for the 30 employees who separated from EOG employment during the period December 2020 through January 2022 to determine whether user access privileges to the OPB network were timely disabled upon an employee's separation from EOG employment.
    - Inquired of OPB management and selected and examined OPB records for 18 of the 200 BAPS change requests made during the period November 2020 through January 2022 to determine whether OPB records evidenced that the changes were appropriately authorized, reviewed and tested, approved, and implemented into production.
    - Inquired of EOG management and examined EOG records to determine whether EOG security controls related to employee use of mobile devices ensured the confidentiality, integrity, and availability of EOG data and IT resources.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.

- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

RON DESANTIS
GOVERNOR

STATE OF FLORIDA
Office of the Governor
THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001
www.flgov.com
850-717-9418

July 16, 2024

Sherrill F. Norman
State of Florida Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Thank you for the opportunity to respond to your preliminary and tentative findings and recommendations for the *Operational Audit of the Executive Officer of the Governor, State Budgetary Processes and Information Technology Controls*.

Our enclosed response fulfills the requirements of our agency to timely respond, as required by Section 11.45(4)(d), Florida Statutes.

We appreciate the efforts of you and your staff in assisting to improve our operations and information systems. Should you have any additional questions regarding our response, please contact my office.

Sincerely,

Brandi Gunder
Deputy Budget Director

Enclosure

cc: Daniel Pardo, Deputy Director of Policy
Melinda Miguel, Chief Inspector General
Michael Jones, Office of Policy & Budget, System Development & Design
Steven Henry, Director of Auditing

EOG Operational Audit:
State Budgetary Processes and Information Technology Controls

Response to Preliminary and Tentative Audit Findings

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.

OPB/SDD Response:

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.

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.

OPB/SDD Response:

SDD will enhance security controls in the recommended areas to provide increased protection to the LAS/PBS environment.

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.

OPB/SDD Response:

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.

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.

OPB/SDD Response:

SDD understands and accepts the risks associated with the current mobile device policy. No change in policy will be made at this time.