STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2021-059
November 2020

EXECUTIVE OFFICE OF THE GOVERNOR

Information Technology Controls
Prior Audit Follow-Up

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 following Governors served during the period of our audit:

The Honorable Ron DeSantis from January 8, 2019
The Honorable Rick Scott to January 8, 2019

The team leader was Randall Nelson, CPA, and the audit was supervised by Karen Van Amburg, CPA.

Please address inquiries regarding this report to Karen 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

Information Technology Controls Prior Audit Follow-Up

SUMMARY

This operational audit of the Executive Office of the Governor (EOG) focused on selected administrative activities and included a follow-up on the findings noted in our report No. 2017-213 related to information technology (IT) controls. Our audit disclosed the following:

Information Technology Controls

Finding 1: The EOG did not always ensure that Information Security Manager appointments were timely made and reported in accordance with State information security laws and rules. A similar finding was noted in our report No. 2017-213.

Finding 2: As similarly noted in our report No. 2017-213, EOG records did not always evidence that EOG employees completed initial security awareness training in accordance with State information security rules.

Finding 3: EOG controls continue to need improvement to ensure that Office of Policy and Budget (OPB) network access privileges are timely disabled upon an employee's separation from EOG employment.

Finding 4: EOG records did not always evidence that Budget Amendment Processing System programming changes were appropriately authorized, reviewed and tested, and approved. Similar findings have been noted in prior audit reports, most recently in our report No. 2017-213.

Finding 5: Security controls over mobile device utilization need improvement to ensure the confidentiality, integrity, and availability of EOG and OPB data and IT resources. A similar finding was communicated in our report No. 2017-213.

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 2019-20 fiscal year, the Legislature appropriated approximately $29.5 million to the EOG and authorized 276 positions.[3]

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

[2] Section 14.201, Florida Statutes.

[3] Chapter 2019-115, Laws of Florida.

FINDINGS AND RECOMMENDATIONS

INFORMATION TECHNOLOGY CONTROLS

State law[4] requires State agencies to establish information security controls to ensure the security of agency data, information, and information technology (IT) resources. Additionally, Agency for State Technology (AST) rules[5] established minimum security standards for ensuring the confidentiality, integrity, and availability of State agency data, information, and IT resources.

The 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 Development and Design Policy Unit (SDD), was responsible for administering a separate network that included OPB applications and systems, including the OPB e-mail system.

Finding 1: Information Security Program Administration

State law[6] requires each State agency head to appoint an Information Security Manager (ISM) to administer the agency's information security program. State agencies were to provide this designation to the AST annually in writing by January 1.[7] Among other things, the ISM is responsible for all agency information security policies, procedures, standards, and guidelines, as well as information security awareness and disaster recovery programs.

As part of our audit, we performed inquiries of EOG management and examined EOG records related to ISM appointments. As similarly noted in our report No. 2017-213 (Finding 1), our audit procedures disclosed that EOG records did not evidence the appointment of an ISM for the 2018 calendar year or that notification was provided to the AST. In addition, the EOG did not notify the AST of the appointment of the ISM for the 2019 calendar year until May 28, 2019, 147 days after the notification was due. According to EOG management, the same individual who was appointed as ISM in 2017 also served as ISM during the 2018 calendar year and the 2019 calendar year until a new ISM was appointed in May 2019, and EOG management was not aware that ISM appointments and notifications were to be done on an annual basis.

Timely ISM appointments in accordance with State law promotes accountability for the administration of the EOG information security program.

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

[5] AST Rules, Chapter 74-2, Florida Administrative Code. Effective July 1, 2019, Chapter 2019-118, Laws of Florida, created the Division of State Technology (DST) within the Department of Management Services (DMS) and transferred the existing powers, duties, functions, personnel, records, property, and funds of the AST to the DST. As of July 1, 2019, AST Rules, Chapter 74-2, Florida Administrative Code, were transferred to DMS Rules, Chapter 60GG-2, Florida Administrative Code. AST Rules, Chapter 74-2, Florida Administrative Code, were in effect during our audit period (July 2017 through April 2019). Effective July 1, 2020, the DST was abolished, and the Florida Digital Service was established in its place.

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

[7] The designation was to be provided to the AST prior to July 2019 and to the DMS annually thereafter.

Recommendation: We again recommend that EOG management ensure that ISM appointments are timely made and reported in accordance with State information security laws and rules.

Finding 2: Security Awareness Training

Effective security awareness programs include initial training for new employees and periodic refresher training for all employees. AST rules[8] required State agencies to provide workers[9] initial security awareness training within 30 days of employment and that, at a minimum, workers receive annual security awareness training. Initial security awareness training was to include, among other things, instruction on acceptable use restrictions, procedures for handling confidential and exempt information, and computer security incident reporting procedures.

In our report No. 2017-213 (Finding 2), we noted that EOG records did not evidence that EOG personnel completed initial security awareness training or were provided annual security awareness training in accordance with AST rules. As part of our follow-up audit procedures, we performed inquiries of EOG management and examined EOG records to determine whether the EOG had established and maintained a security awareness training program in accordance with applicable rules. Our examination of EOG records for 11 of the 83 employees hired during the period July 10, 2018, through April 20, 2019, disclosed that 4 employees did not complete security awareness training within 30 days of hire. Specifically, 2 of the employees completed security awareness training 115 and 156 days after hire and the other 2 employees had not completed security awareness training as of August 30, 2019, 233 and 210 days after hire. According to EOG management, EOG policies and procedures did not provide effective mechanisms for ensuring that employees completed required training.

The timely completion of security awareness training by EOG personnel provides management greater assurance that employees will adequately understand and be aware of EOG information security requirements and serves to demonstrate compliance with applicable information security rules.

Recommendation: We recommend that EOG management strengthen policies and procedures to ensure that all personnel timely complete security awareness training in accordance with applicable information security rules.

Finding 3: OPB Network Access Privilege Controls

AST rules[10] required State agencies to ensure that IT access privileges were removed when access to an IT resource was no longer required. Prompt action to deactivate access privileges when an employee separates from employment or access to the IT resource is no longer required is necessary to help prevent misuse of the access privileges.

[8] AST Rule 74-2.003(3)(b) and (c), Florida Administrative Code.

[9] AST Rule 74-2.001(3)(a)33., Florida Administrative Code, defined workers as members of the workforce who may or may not use IT resources and included employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, was under the direct control of the agency, whether or not they were paid by the agency.

[10] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

As part of our audit, we compared People First[11] records to EOG network disablement date records for 8 of the 23 employees who separated from EOG employment during the period January 2018 through April 2019. Our comparison found that the EOG did not always promptly disable user network access privileges when employees separated from EOG employment. Specifically, network access privileges for 5 of the employees remained active 8 to 142 business days (an average of 59 business days) after the employees' separation dates. According to EOG management, leadership transition and communication issues contributed to the untimely disabling of user network access privileges.

As unauthorized access can occur at any time, promptly disabling user network access privileges reduces the risk that access privileges may be misused by the former employee or others. A similar finding was noted in our report No. 2017-213 (Finding 4).

Recommendation: We recommend that EOG management continue to enhance procedures to ensure that network access privileges are immediately disabled upon a user's separation from EOG employment.

Finding 4: Configuration Management Controls

To promote effective configuration management over IT resources, AST rules[12] required State agencies to establish a configuration management process to manage upgrades and modifications to existing IT resources. Effective configuration management controls ensure that all configuration changes (program or functionality changes) follow a configuration management process that provides for an appropriate separation of duties and ensures changes are appropriately authorized, reviewed and tested, and approved. Additionally, agency controls should clearly document and track the configuration management process from initial authorization of the change to final approval.

The SDD utilized Visual Studio Team Foundation Server (TFS) software to track changes to the Budget Amendment Processing System (BAPS) and to document, for each change, the identity of the requestor, programmer, and tester. As part of our audit, we inquired of SDD management and examined TFS records for 7 of the 42 BAPS change requests made during the period July 2017 through April 2019 and noted that EOG records did not evidence that 2 of the changes were independently tested and for 1 of these changes, EOG records also indicated that the same individual authorized, reviewed, and approved the change. In response to our audit inquiry, EOG management indicated that staff shortages and OPB workload issues caused the lack of separation of duties and absence of independent testing.

The proper separation of configuration management duties and independent reviews of BAPS changes strengthen the effectiveness of SDD configuration management controls by ensuring that changes are accurate and appropriate. Similar findings were noted in our report Nos. 2017-213 (Finding 6) and 2014-200 (Finding 5).

Recommendation: We recommend that EOG management enhance configuration management controls to ensure that TFS records demonstrate that BAPS programming changes are appropriately authorized, reviewed and tested, and approved.

[11] People First is the State's human resource information system.

[12] AST Rule 74-2.003(5)(c), Florida Administrative Code.

Finding 5: Mobile Device Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to mobile device[13] utilization need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising EOG and OPB data and IT resources. However, we have notified appropriate EOG and OPB management of the specific issues.

Without appropriate security controls related to the use of mobile devices by EOG employees, the risk is increased that the confidentiality, integrity, and availability of EOG and OPB data and IT resources may be compromised. A similar finding was noted in our report No. 2017-213 (Finding 8).

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

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. 2017-213.

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 June 2019 through September 2020 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 selected administrative activities. The overall 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 assigned responsibilities in accordance with applicable laws, administrative rules, contracts, grant agreements, and other guidelines.
- To examine internal controls designed and placed in 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.

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

- To 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. 2017-213.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, deficiencies in management's internal controls, 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; 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, 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 selected EOG administrative processes.
- Performed inquiries of EOG personnel and examined EOG records to determine whether the EOG properly accounted for tangible personal property. Specifically, we examined EOG records for:
    - 10 tangible personal property items with acquisition costs totaling $38,891 selected from the population of 60 tangible personal property items with acquisition costs totaling $131,502, acquired during the period July 2017 through April 2019.
    - 10 tangible personal property items with acquisition costs totaling $18,962 selected from the population of 34 tangible personal property items with acquisition costs totaling $62,367, disposed of during the period July 2017 through April 2019.

- 25 tangible personal property items with acquisition costs totaling $118,268 selected from the population of 232 tangible personal property items with acquisition costs totaling $635,658, that were active as of April 30, 2019.

- Determined whether EOG administrative and travel expenditures were properly recorded, supported, and made in accordance with applicable laws, rules, and other guidelines. Specifically, we examined EOG records for:
  - 40 general expenditure payments totaling $305,026 selected from the population of 7,092 general expenditure payments totaling $8,242,010, made during the period July 2017 through April 2019.
  - 40 purchasing card transactions totaling $25,683 selected from the population of 3,828 purchasing card transactions totaling $318,890, made during the period July 2017 through April 2019.
  - 40 travel expenditure transactions totaling $20,274 selected from the population of 5,654 travel expenditure transactions totaling $742,541, made during the period July 2017 through April 2019.
  - 15 contractual purchases totaling $439,750 selected from the population of 65 contractual purchases totaling $681,404, made during the period July 2017 through April 2019.
- Evaluated EOG actions to correct the findings noted in our report No. 2017-213. Specifically, we:
  - Examined EOG records related to Information Security Manager appointments for the 2018 and 2019 calendar years to determine whether the EOG complied with Section 281.318(4)(a), Florida Statutes, and Agency for State Technology (AST) Rule 74-2.002(1)(f)8., Florida Administrative Code.
  - Performed inquiries of EOG management and examined EOG records to determine whether the EOG appropriately implemented and maintained a security awareness training program in accordance with AST rules. Specifically, we selected and examined EOG records related to 11 of the 83 employees hired during the period July 10, 2018, through April 20, 2019, to determine whether the employees completed security awareness training within 30 days of hire.
  - Performed inquiries of EOG management and examined EOG records to determine whether EOG management designated positions of special trust in accordance with Section 110.1127(2)(a), Florida Statutes, and whether, as a condition of continued employment, the EOG conducted level 2 background screenings for all employees in positions of special trust.
  - Performed inquiries of Office of Policy and Budget (OPB) management and selected and examined OPB records for 8 of the 23 employees who separated from EOG employment during the period January 2018 through April 2019 to determine whether OPB records demonstrated that OPB network access privileges were timely disabled upon an employee's separation from EOG employment.
  - Performed inquiries of OPB management and examined OPB records to determine whether OPB management performed periodic reviews of user access privileges to the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem and the Budget Amendment Processing System to verify the continued appropriateness of assigned user access privileges.
  - Performed inquiries of OPB management and examined OPB records to determine whether OPB management enhanced security controls related to the logging and monitoring of OPB network and related application activities to ensure the confidentiality, integrity, and availability of OPB data and information technology (IT) resources.

- Performed inquiries of OPB management and selected and examined OPB records for 7 of the 42 BAPS change requests made during the period July 2017 through April 2019 to determine whether OPB records evidenced that the changes were appropriately authorized, reviewed and tested, and approved.
- Performed inquiries of EOG management and examined EOG records to determine whether EOG mobile device authorization controls ensured that, for all users of agency-owned and agency-managed mobile devices, EOG records included user agreement forms approved in accordance with EOG policy.
- Performed inquiries of EOG and OPB management and examined EOG and OPB records to determine whether EOG and OPB security controls related to employee use of mobile devices ensured the confidentiality, integrity, and availability of EOG and OPB data and IT resources.

- Reviewed applicable laws, rules, and other State guidelines to obtain an understanding of the legal framework governing EOG operations.
- Interviewed EOG management, examined EOG forms, and evaluated EOG compliance with applicable statutory requirements for collecting and utilizing individuals' social security numbers.
- Observed, documented, and evaluated the effectiveness of selected EOG processes and procedures for:
  - Cash and revenue management, purchasing activities, managing FLAIR and other IT system access privileges, settlement agreements, and fixed capital outlay.
  - The acquisition and management of real property leases in accordance with State law, Department of Management Services rules, and other applicable guidelines. As of June 2018, the EOG was responsible for five real property leases.
- 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

November 23, 2020

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 based on your audit of the Executive Office of the Governor - Operational Audit - Information Technology Controls Prior Audit Follow-Up. Please find attached your preliminary and tentative findings document dated November 3, 2020 and our incorporated response as requested.

Many thanks to you and your staff for your continued efforts to further State of Florida accountability and government transparency. Should you have any additional questions regarding our response, please contact my office.

Sincerely,

Dawn Hanson
Director of Administration

cc: Melinda Miguel, Chief Inspector General
Rodney MacKinnon, Director of Auditing

Attachment: Preliminary and Tentative Finding Response

Finding 1: Information Security Program Administration

The Executive Office of the Governor (EOG) did not always ensure that Information Security Manager (ISM) appointments were timely made and reported in accordance with State information security laws and rules. A similar finding was noted in Auditor General Report No. 2017-213.

Recommendation: We recommend that EOG management ensure that ISM appointments are timely made and reported in accordance with State information security laws and rules.

Management Response: We concur with your finding and have enhanced our policies and procedures to ensure timely submission of an annual appointment letter. We have noted our procedures that an annual appointment letter is be to submitted regardless of change in position.

Finding 2: Security Awareness Training

As similarly noted in Auditor General Report No. 2017-213, EOG records did not always evidence that EOG employees completed initial security awareness training in accordance with State information security rules.

Recommendation: We recommend that EOG management strengthen policies and procedures to ensure that all personnel timely complete security awareness training in accordance with applicable information security rules.

Management Response: We concur with your finding. We have implemented security awareness training throughout the EOG and will update the timing of our annual security refresher training to encourage full compliance. Additionally, we will strengthen our internal policies regarding completion of training by EOG employees.

Finding 3: OPB Network Access Privilege Controls

EOG controls continue to need improvement to ensure that Office of Policy and Budget (OPB) network access privileges are timely disabled upon employee's separation from EOG employment.

Recommendation: We recommend that EOG management continue to enhance procedures to ensure that network access privileges are immediately disabled upon a user's separation from EOG employment.

Management Response: We concur with your finding. Procedures have been modified to enhance the timeliness and accuracy of the termination notices and termination requests from the Office of Policy and Budget.

Finding 4: Configuration Management Controls

EOG records did not always evidence that Budget Amendment Processing System programming changes were appropriately authorized, reviewed and tested, and approved. Similar findings have been noted in prior audit reports, most recently in AG Report No. 2017-213.

Recommendation: We recommend that EOG management enhance configuration management controls to ensure that TFS records demonstrate that BAPS programming changes are appropriately authorized, reviewed and tested, and approved.

Management Response: We concur with your finding, and we have revised internal procedures to better document change requests, authorization, and completion. We recognize your concerns regarding system revision controls; however, due to the size of our organization, certain multi-tiered reviews and approvals are not always possible. We will make every effort to enhance documentation as a compensating control regarding authorization, review and testing, and approvals.

Finding 5: Mobile Device Security Controls

Security controls over mobile device utilization need improvement to ensure the confidentiality, integrity, and availability of EOG and OPB data and IT resources. A similar finding was communicated in AG Report No. 2017-213.

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

Management Response: We concur with your finding. While we believe that our security controls related to mobile devices are sufficient to ensure confidentiality, integrity and availability of EOG/OPB data and related IT resources, we recognize your concerns and recommendation and will continue to monitor security controls related to mobile devices.