STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2017-213
June 2017

# EXECUTIVE OFFICE OF THE GOVERNOR

## Information Security Controls and Mobile Device Management


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 Rick Scott served as Governor during the period of our audit.

The team leader was Clint Boutwell, CPA, and the audit was supervised by Jane Flowers, CPA.

Please address inquiries regarding this report to Matthew Tracy, CPA, Deputy Auditor General, by e-mail at matthewtracy@aud.state.fl.us or by telephone at (850) 412-2922.

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 Security Controls and Mobile Device Management

## *SUMMARY*

This operational audit of the Executive Office of the Governor (EOG) focused on information security controls, mobile device management, and the Office of Open Government. Our audit also included a follow-up on the findings noted in our report No. 2014-200. Our audit disclosed the following:

### Information Security 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. Additionally, EOG management and management of the Office of Policy and Budget (OPB) within the EOG should work together to better ensure that the risks related to the OPB e-mail and other information technology (IT) systems are appropriately considered and subject to sufficient and appropriate oversight.

**Finding 2:** EOG records did not evidence that EOG personnel completed initial security awareness training or were provided annual security awareness training in accordance with Agency for State Technology rules.

**Finding 3:** The EOG did not always ensure that IT personnel whose duties placed them in positions of special trust were subject to required background screenings.

**Finding 4:** OPB records did not evidence that OPB network access privileges were timely deactivated upon an employee's separation from EOG employment or that periodic reviews of user access privileges to the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem or the Budget Amendment Processing System (BAPS) were conducted.

**Finding 5:** Certain security controls related to logging and monitoring of OPB network and application activities need improvement to ensure the confidentiality, integrity, and availability of OPB data and related IT resources.

**Finding 6:** As similarly noted in our report No. 2014-200, OPB records did not evidence independent review and testing of BAPS programming changes.

### Mobile Device Management

**Finding 7:** EOG records did not always evidence that mobile device users had been appropriately authorized to access the EOG or OPB e-mail systems in accordance with EOG policies.

**Finding 8:** Security controls over mobile device utilization need improvement to ensure the confidentiality, integrity, and availability of EOG and OPB data and related 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 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 2015-16 fiscal year, the Legislature appropriated approximately $28.3 million to the EOG and authorized 276 positions.

# FINDINGS AND RECOMMENDATIONS

## INFORMATION SECURITY CONTROLS

State law[3] 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[4] establish 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 for those of 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[5] and AST rules[6] require each State agency head to appoint an Information Security Manager (ISM) to administer the agency's information security program. Prior to March 2016, State agencies were required to inform the State Chief Information Security Officer (CISO) in writing of the appointment within 1 week of the effective date of the appointment, and annually thereafter 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.

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

[2] Section 14.201, Florida Statutes.

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

[4] AST Rules, Chapter 74-2, Florida Administrative Code. Although AST Rules were not effective until March 2016, the AST's predecessor agency, the Agency for Enterprise Information Technology (AEIT), promulgated similar IT security requirements in AEIT Rules, Chapters 71A-1 and 71A-2, Florida Administrative Code.

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

[6] AST Rule 74-2.002(1)(f)8., Florida Administrative Code. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.003, Florida Administrative Code, also required State agency heads to appoint an ISM to administer the agency's information security program.

[7] Pursuant to Section 282.318(4)(a), Florida Statutes, and AST Rule 74-2.002(1)(f)8., Florida Administrative Code, effective March 2016, State agencies are required to report ISM appointments and reappointments in writing each year to the AST by January 1.

The EOG assigned ISM responsibilities to the Director of the OIS, who also served as the EOG Chief Information Officer. The EOG *Computer Security Policy* specified that the EOG ISM was responsible for the overall development, implementation, administration, and coordination of the EOG information security program. As part of our audit, we performed inquiries of EOG and OPB management and examined EOG records related to ISM appointments and the EOG information security program. Our audit procedures disclosed that:

- Although the EOG had assigned ISM responsibilities to the Director of the OIS, EOG records did not evidence the formal appointment of an ISM for the 2014 calendar year or that notification of an ISM appointment was provided to the State CISO. In addition, the EOG did not provide the State CISO notice of the appointment of the ISM for the 2015 calendar year until April 1, 2015, 90 days after the written notification was due. Additionally, while the EOG appointed a new ISM on November 9, 2015, the EOG did not provide the State CISO notice of the appointment until July 25, 2016, subsequent to our audit inquiry and 252 days after written notification was due.
- The EOG information security program did not encompass the OPB IT or e-mail systems and, consequently, did not account for risks related to the OPB e-mail and other IT systems. Our examination of the EOG 3-year comprehensive risk assessment submitted to the AST[8] in 2014 also disclosed that the risk assessment did not consider OPB e-mail or other IT systems.

  In response to our audit inquiries, the EOG ISM indicated that OPB SDD network administrators were responsible for OPB e-mail and other IT systems and OPB management indicated that the OPB adhered to EOG information security policies. Both the EOG and OPB management also indicated that, because the OPB SDD and Legislature jointly administered the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem (LAS/PBS) and the OPB SDD administered the Budget Amendment Processing System (BAPS) that interfaced with the LAS/PBS, providing the EOG ISM access to and oversight of OPB IT systems was not advisable. However, both EOG and OPB management further indicated that they would consider appointing an OPB Security Representative to coordinate OPB IT security procedures with the EOG ISM.

  While the management of the LAS/PBS and BAPS presents unique separation of powers considerations, as the OPB is an EOG organizational unit, it is critical that equivalent compensating controls,[9] such as the appointment of an OPB Security Representative, be established to ensure that the risks related to the OPB e-mail and other IT systems are considered and mitigated in accordance with State information security rules.

Formal and timely ISM appointments promote accountability for the administration of the EOG information security program. Additionally, the establishment of equivalent compensating security controls for the OPB e-mail and other IT systems would promote consistency with State information security rules and better ensure that the risks associated with the OPB IT systems and resources are appropriately considered and the systems are subjected to sufficient and appropriate oversight.

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

[8] Section 282.318, Florida Statutes, requires State agencies to conduct, and update every 3 years, a comprehensive risk assessment of security threats to agency data, information, and IT resources, and submit the completed assessment to the AST.

[9] AST Rule 74-2.001(3)(a)4., Florida Administrative Code, defined compensating controls as management, operational, and/or technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of required security controls that provide equivalent or comparable protection for an IT resource. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.002(20), Florida Administrative Code, similarly defined compensating controls.

**compensating controls are established to mitigate the risks related to the OPB e-mail and other IT systems and to subject the systems to sufficient and appropriate oversight.**

## Finding 2: Security Awareness Training

Effective security awareness programs include initial training for new employees and periodic refresher training for all employees. AST rules[10] require State agencies to provide workers[11] initial security awareness training within 30 days of employment and that, at a minimum, workers receive annual security awareness training. Initial security awareness training is to include, among other things, instruction on acceptable use restrictions, procedures for handling confidential and exempt information, and computer security incident reporting procedures.

As part of our audit, 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 audit procedures disclosed that EOG records did not evidence that EOG personnel completed initial security awareness training or were provided annual security awareness training. Specifically, we noted that:

- While the EOG e-mailed new employees hyperlinks to EOG policies and training materials that included guidelines on acceptable computer use, handling confidential and exempt information, and reporting certain computer security incidents, the e-mails did not instruct employees to review the policies or training materials within 30 days of employment. In addition, EOG records did not evidence that new employees reviewed the policies or training materials.
- EOG records did not evidence that employees had been provided annual security awareness training during the period July 2014 through March 2016.

The completion of initial and ongoing 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 AST security awareness training rules.

**Recommendation: We recommend that EOG management establish a comprehensive and documented security awareness training program in accordance with AST rules.**

## Finding 3: Background Screenings

State law[12] requires State agencies to designate those positions that, because of the special trust, responsibility, or sensitive location of those positions, require background screenings. State law specifies that all employees in such positions, as a condition of employment and continued employment, be subject

[10] AST Rule 74-2.002(3)(b) and (c), Florida Administrative Code. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.008(2) and (3), Florida Administrative Code, specified similar requirements.

[11] AST Rule 74-2.001(3)(a)21., Florida Administrative Code, defines workers as members of the workforce who may or may not use IT resources. Workers include employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency.

[12] Section 110.1127(2)(a), Florida Statutes.

to level 2 background screenings.[13] Additionally, AST rules[14] specify that State agencies are responsible for performing background checks for all individuals hired as IT workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate-impact or higher.

We noted that, although the EOG had not designated positions of special trust, effective March 7, 2011, the EOG required all new employees to undergo level 2 background screenings as a condition of employment. Our examination of EOG records for 20 of the 46 OIS and SDD IT employees whose duties during the period July 2014 through March 2016 placed them in positions of special trust disclosed that the EOG did not always ensure that employees were subject to required level 2 background screenings. Specifically, EOG records did not evidence that 8 of the 20 employees had been subject to a level 2 background screening as a condition of employment or continued employment. In response to our audit inquiry, EOG management indicated that the employees had not been subject to background screenings because the employees were hired before March 7, 2011, and, based on EOG legal counsel advice, the EOG had not conducted background screenings on employees hired before that date. Notwithstanding management's response, since July 1, 2012, State law has required that all employees who serve in positions of special trust be subject to level 2 background screenings as a condition of continued employment.

Performing level 2 background screenings on all employees whose duties place them in positions of special trust provides management assurance that only those individuals with appropriate backgrounds are granted access to EOG data and IT resources.

**Recommendation: We recommend that EOG management designate positions of special trust and ensure that, as a condition of employment and continued employment, level 2 background screenings are performed and documented for all employees whose duties place them in positions of special trust.**

## Finding 4: OPB Network and System Access Privilege Controls

AST rules[15] require State agencies to ensure that IT access privileges are removed when access to an IT resource is 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. AST rules[16] also require State agencies to periodically review user access privileges for appropriateness. Periodic reviews of user access privileges help ensure that

[13] Pursuant to Section 435.04, Florida Statutes, level 2 background screenings are to include, but need not be limited to, fingerprinting for Statewide criminal history records checks through the Department of Law Enforcement, national criminal history records checks through the Federal Bureau of Investigation, and may include local criminal records checks through local law enforcement agencies.

[14] AST Rule 74-2.002(1)(f)9., Florida Administrative Code. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.004(1), Florida Administrative Code, advised State agency heads to designate IT positions with access to information technology processing facilities and certain system, developer, network, or other administrative capabilities as positions of special trust.

[15] AST Rule 74-2.003(1)(a)8., Florida Administrative Code. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.007(6), Florida Administrative Code, required access authorization be promptly removed when the user's employment was terminated or access to the information resource was no longer required.

[16] AST Rule 74-2.003(1)(a)6., Florida Administrative Code. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.007(2), Florida Administrative Code, specified similar requirements.

only authorized users have access to IT resources and that the access provided to each user remains appropriate.

As part of our audit, we evaluated certain user access privilege controls, including those for the OPB network and selected systems. Our audit procedures disclosed that:

- OPB records did not evidence the timely deactivation of OPB network access privileges for 10 of the 59 employees who separated from EOG employment during the period July 2014 through March 2016. In response to our audit inquiry, SDD management indicated that OPB network accounts are deleted when an employee separates from EOG employment. Consequently, access control records demonstrating the dates that the employees' access privileges were deactivated were not available. Maintaining historical access control records would better demonstrate that network access privileges are timely deactivated upon an employee's separation from EOG employment and would assist in future investigations of security incidents, should they occur.
- OPB records did not evidence periodic reviews of user access privileges to the LAS/PBS or BAPS. Without periodic reviews of user access privileges, the risk is increased that unauthorized or inappropriate access privileges may exist and not be timely detected.

**Recommendation: We recommend that OPB management retain OPB network access control records sufficient to demonstrate that user access privileges are timely deactivated upon an employee's separation from EOG employment or when the access privileges are no longer required. We also recommend that OPB management perform periodic reviews of user access privileges to the LAS/PBS and BAPS to verify the continued appropriateness of assigned user access privileges.**

## Finding 5: Security Controls – Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to logging and monitoring of OPB network and related application activities needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising OPB data and related IT resources. However, we have notified appropriate OPB management of the specific issues. Without appropriate security controls related to logging and monitoring of OPB network and application activities, the risk is increased that the confidentiality, integrity, and availability of OPB data and related IT resources may be compromised.

**Recommendation: We recommend that OPB management enhance certain security controls related to logging and monitoring of OPB network and related application activities to ensure the confidentiality, integrity, and availability of OPB data and related IT resources.**

## Finding 6: Configuration Management Controls

To promote effective configuration management over IT resources, AST rules[17] require 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

[17] AST Rule 74-2.003(5)(c), Florida Administrative Code. Although AST Rules were not effective until March 2016, AEIT Rule 71A-1.011(4), Florida Administrative Code, specified a similar requirement.

appropriate separation of duties and ensures changes are appropriately authorized, reviewed and tested, and approved. Additionally, agency records 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 BAPS and to document, for each change, the identity of the requestor, programmer, and tester. While the TFS software automatically identified the SDD programmers involved with change requests and provided programmers the ability to manually identify what configuration management function each programmer's actions related to, the software did not automatically identify the configuration management functions performed.

In our report No. 2014-200 (finding No. 5), we noted that the EOG could not always demonstrate that changes to BAPS were properly authorized, tested, and approved. As part of our audit follow-up procedures, we inquired of SDD management and examined TFS records for 5 of the 334 BAPS change requests made during the period July 2014 through March 2016 and noted that the SDD programmers had not manually identified the configuration management functions performed. Consequently, for the 5 BAPS change requests subject to audit testing, TFS records did not evidence independent review and testing of the changes.

Independent review and testing of BAPS changes strengthens the effectiveness of SDD configuration management controls by ensuring that changes are accurate and appropriate.

**Recommendation: We recommend that OPB management enhance configuration management controls to ensure that TFS records demonstrate that all BAPS programming changes are subject to independent review and testing.**

## MOBILE DEVICE MANAGEMENT

Pursuant to the EOG Mobile Device Policy (Policy), the use of mobile devices (cellular telephones or smartphones) by EOG employees was to be limited to employees who:

- As part of their official assigned duties, must routinely be immediately available to citizens, supervisors, or subordinates;
- Must be available to respond to emergency situations;
- Must be available to calls outside of regular working hours;
- Needed access to the technology to productively perform job duties in the field; or,
- Had limited or no access to a standard phone.

In accordance with the Policy, the EOG maintained procedures that allowed authorized employees to utilize agency-owned and agency-managed mobile devices to perform their official responsibilities. Agency-owned mobile devices were the property of the EOG, which managed the devices to ensure that the devices' hardware and software met EOG security requirements. Agency-managed mobile devices were employee-owned devices that the EOG required to be enrolled in the EOG Mobile Device Management program to ensure compliance with EOG security and access standards.

Users of both agency-owned and agency-managed devices were required to agree to EOG security requirements through the completion of a standard user agreement form (UA form). The Policy

incorporated all EOG IT and security policies through reference and was applicable to users of both OIS and OPB-administered e-mail and IT systems. Mobile device user access to EOG IT resources was limited to employee e-mails.

## Finding 7: Mobile Device Authorizations

Pursuant to the Policy, all requests for agency-owned mobile devices were to be submitted to the EOG, Office of Administration, by the Director of the applicable EOG unit. Employee use of an agency-owned mobile device required a UA form approved by the EOG Chief of Staff (or designee). Employee use of an agency-managed mobile device required a UA form approved by the Director of the OIS. Employee access to the OPB e-mail system through either an agency-owned or agency-managed mobile device also required a UA form approved by the OPB Director (or designee). To evaluate whether EOG procedures adequately ensured that only authorized employees participated in the EOG mobile device program we:

- Obtained and compiled listings of the mobile devices (agency-managed and agency-owned) that accessed either the OIS e-mail system during the period July 2015 through August 2016 or the OPB e-mail system during the period October 2015 through August 2016 and evaluated whether EOG records included appropriately approved UA forms for the users of these mobile devices. Our audit procedures disclosed that EOG records did not include a UA form for the users of 9 of the 151 agency-managed mobile devices and the users of 2 of the 43 agency-owned mobile devices that accessed either the OIS or OPB e-mail systems. In response to our audit inquiry, OIS and SDD management indicated that users are not required to complete a UA form for new or replacement devices, which may have contributed to UA forms not always being available.
- Examined the UA forms for employees who used agency-owned or agency-managed mobile devices during the period July 2014 through March 2016 to determine whether the employees' use of the devices had been authorized in accordance with the Policy. Our examination disclosed that 118 of the 137 UA forms included in EOG records did not evidence that the appropriate member of management or their designee had signed the UA form authorizing the employee's use of the device. In response to our audit inquiry, OIS management indicated that the OIS would evaluate and revise procedures to ensure appropriate approvals are obtained and documented. Additionally, OPB management indicated that, although the SDD Director had routinely approved UA forms for SDD users, no documented delegation of authority was available.

Appropriately approved UA forms for all mobile device users demonstrate that only authorized employees access the OIS and OPB e-mail systems.

**Recommendation: We recommend that EOG management enhance mobile device authorization controls to ensure that, for all users of agency-owned and agency-managed mobile devices, EOG records evidence UA forms approved in accordance with the Policy.**

## Finding 8: Mobile Device Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed certain security controls related to mobile device utilization that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising EOG and OPB data and related 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 related IT resources may be compromised.

**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 related IT resources.**

## PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2014-200.

## 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 March 2016 through November 2016 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 information security controls, mobile device management, and the Office of Open Government (OOG). 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 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.
- 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. 2014-200.

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 gain an understanding of EOG information security controls.
- Performed inquiries of EOG personnel and examined EOG records to determine whether EOG management had adequately designed and implemented controls, including policies and procedures, for information security.
- Performed inquiries of EOG personnel and examined EOG records to determine whether the OOG had established and maintained an appropriate information security awareness training program during the period July 2014 through March 2016.
- Performed inquiries of EOG and Office of Policy and Budget (OPB) management, observations, and examined EOG and OPB records to determine whether adequate controls for agency-owned and agency-managed mobile devices had been established during the period July 2014 through March 2016.
- Examined mobile device user agreements and other EOG records to determine whether the EOG had established effective controls for authorizing the use of agency-owned and agency-managed mobile devices and ensuring that EOG data and records subject to public records requests were retained and protected in accordance with applicable laws, rules, and other guidelines.
- Performed inquiries of OPB management and examined OPB network access control records for 10 of the 59 employees who separated from EOG employment and whose network access privileges were deactivated during the period July 2014 through March 2016 to determine whether the OPB had established sufficient controls to ensure that access privileges were timely deactivated upon an employee's separation from EOG employment.
- Performed inquiries of OPB management and examined applicable Systems Development and Design Policy Unit (SDD) Service Request forms for 15 of the 84 network user accounts that were

active as of August 22, 2016, to determine whether access to the network was limited to authorized personnel.

- Performed inquiries of EOG and OPB management, examined selected records, and compared EOG and OPB disaster recovery plans for the period July 2014 through March 2016 to State information security rules to determine whether the EOG and OPB had established appropriate controls to ensure the timely recovery of EOG and OPB data and records.
- Examined EOG records for 20 of the 46 OIS and SDD employees whose duties during the period July 2014 through March 2016 placed them in positions of special trust to determine whether the EOG had established sufficient controls to ensure that personnel responsible for the administration of EOG information security controls met all position qualifications, received required training, and were subject to level 2 background screenings as a condition of employment and continued employment.
- Performed inquiries of EOG management and observations and examined EOG records to determine whether EOG Data Classification standards were sufficient to identify EOG information assets, information asset owners, custodians, security classifications, recovery priority, organizational value, and legal hold status.
- Examined documentation related to 5 of the 33 information technology (IT) related third-party agreements effective during the period July 2014 through March 2016 to determine whether the EOG had established sufficient controls to ensure all identified risks were considered and corresponding information security controls were included in third-party agreements to protect EOG information assets or provide indemnification in case of loss.
- Reviewed applicable laws, rules, and other guidelines to obtain an understanding of the legal framework governing EOG operations.
- Interviewed EOG management, examined selected EOG records, and evaluated EOG compliance with applicable statutory requirements for collecting and utilizing individuals' social security numbers.
- Performed inquiries of EOG management and examined EOG records to determine whether the EOG had timely performed FLAIR user access privileges reviews during the period July 2014 through March 2016 in accordance with EOG policies and procedures and taken appropriate actions to prevent the assignment of incompatible responsibilities.
- Observed, documented, and evaluated the effectiveness of selected EOG processes and procedures for:
    - Budgeting, revenues and cash receipts, cash management, purchasing, settlement agreements, and financial reconciliations.
    - The administration of purchasing cards in accordance with applicable guidelines. As of March 31, 2016, the EOG had 40 active purchasing cards.
    - The administration of EOG contracts in accordance with applicable guidelines. During the period July 2014 through February 2016, the EOG was responsible for 14 active contracts.
    - The assignment and use of motor vehicles. As of March 31, 2016, the EOG was responsible for 3 motor vehicles with recorded acquisition costs totaling $46,509.
    - The assignment and use of wireless devices with related costs totaling $35,817 during the period July 2014 through February 2016.
    - The administration of EOG travel in accordance with State law and other applicable guidelines. During the period July 2014 through February 2016, EOG travel expenditures totaled $380,373.

- The management of tangible personal property. As of February 29, 2016, the EOG was responsible for tangible personal property with acquisition costs totaling $2,751,322.

- Evaluated EOG actions taken to correct the findings noted in our report No. 2014-200. Specifically, we:
  - Examined documentation related to fixed capital outlay (FCO) requests received from 5 of the 30 State agencies who submitted an LBR for the 2015-16 fiscal year and compared the requests to OPB guidelines to determine whether the OPB ensured that State agencies submitted all required forms with FCO requests.
  - Performed inquiries of EOG management, examined EOG records, and observed the OPB Federal Grants Tracking System to determine whether the EOG complied with Section 216.212(1)(a)(2), Florida Statutes, and requirements related to the oversight and coordination of Federal funds.
  - Performed inquiries of EOG management and examined documentation related to 5 of the 2,083 budget amendments processed through the Budget Amendment Processing System (BAPS) during the period July 2014 through March 2016 to determine whether all actions related to processing budget amendments were traceable to the responsible individual.
  - Performed inquiries of OPB management and observations to determine whether OPB management took appropriate corrective actions related to OPB network authentication controls.
  - Performed inquiries of OPB management, observations, and examined documentation related to 5 of the 334 BAPS programming changes and 5 of the 141 Legislative Appropriations Subsystem and Planning and Budgeting Subsystem programming changes made during the period July 2014 through March 2016 to determine whether OPB records evidenced the appropriate separation of configuration change management duties in accordance with applicable rules and other guidelines.
- 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

RICK SCOTT
GOVERNOR

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

June 16, 2017

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 Security Controls and Mobile Device Management. Please find attached your preliminary and tentative findings document dated May 30, 2017 with 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: Eric Miller, Chief Inspector General
Michael Bennett, Director of Auditing

Attachment: Preliminary and Tentative Finding Response

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 1:*** 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. Additionally, EOG management and management of the Office of Policy and Budget (OPB) within the EOG should work together to better ensure that the risks related to the OPB e-mail and other information technology (IT) systems are appropriately considered and subject to sufficient and appropriate oversight.

***Recommendation:*** We recommend that EOG management ensure that ISM appointments are timely made and reported in accordance with State information security laws and rules. We also recommend that EOG management work with OPB management to ensure that appropriate compensating controls are established to mitigate the risks related to the OPB e-mail and other information technology (IT) systems and to subject the systems to sufficient and appropriate oversight.

**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:**

The Information Security Manager appointment for the period of January 1, 2017 to December 31, 2017 was submitted to the Agency of State Technology on January 26, 2017. EOG Information Technology staff agree to communicate with OPB on security related risks and issues. ISM appointments and any necessary delegations will continue to be submitted in a timely manner.

**Projected Completion Date:**
**Contact Person/Phone:** Antony Zoghbi / 850-717-9276

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 2:*** EOG records did not evidence that EOG personnel completed initial security awareness training or were provided annual security awareness training in accordance with Agency for State Technology (AST) rules.

***Recommendation:*** We recommend that EOG management establish a comprehensive and documented security awareness training program in accordance with AST rules.

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

## Management's Current Response

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

**Description of Corrective Action(s) or Explanation of No Action:**

After evaluating several options, EOG intends to conduct security awareness training utilizing a cloud based vendor. All new employees will be required to complete security awareness training within 30 days of hire. All employees will be required to complete the assigned training annually.

**Projected Completion Date:** 7/31/2017
**Contact Person/Phone:** Antony Zoghbi / 850-717-9276

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 3:*** The EOG did not always ensure that IT personnel whose duties placed them in positions of special trust were subject to required background screenings.

***Recommendation:*** We recommend that EOG management designate positions of special trust and ensure that, as a condition of employment and continued employment, level 2 background screenings are performed and documented for all employees whose duties place them in positions of special trust.

**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:**

The EOG personnel office has implemented a process to conduct level 2 background screens on IT personnel in positions of special trust every 3 years. This rescreening requirement has been updated on both the applicable IT staff's position description as well as in PeopleFirst. Additionally, a tracking system has been created to ensure proper screening is done in a timely manner by the personnel office. Once completed, the screens will be placed in the appropriate section of the personnel file.

**Projected Completion Date:**
**Contact Person/Phone:** Dawn Hanson / 850-717-9210

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 4:*** OPB records did not evidence that OPB network access privileges were timely deactivated upon an employee's separation from EOG employment or that periodic reviews of user access privileges to the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem or the Budget Amendment Processing System (BAPS) were conducted.

***Recommendation:*** We recommend that OPB management retain OPB network access control records sufficient to demonstrate that user access privileges are timely deactivated upon an employee's separation from EOG employment or when the access privileges are no longer required. We also recommend that OPB management perform periodic reviews of user access privileges to the Legislative Appropriations Subsystem/Planning and Budgeting Subsystem (LAS/PBS) and BAPS to verify the continued appropriateness of assigned user access privileges.

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

## Management's Current Response

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

**Description of Corrective Action(s) or Explanation of No Action:**

Systems Design and Development (SDD) will no longer delete a local area network user account when a user leaves employment. Network accounts will be deactivated to retain the date and time when security privileges were removed.

LAS/PBS has a report available to security operators that will list all Office of Policy and Budget (OPB) user(s) with access to LAS/PBS. The report includes all elements of the user's security record. SDD recommends OPB run and review the report annually to ensure that only authorized users have access to LAS/PBS.

A report is being created in the BAPS system that will allow security operators to display all elements of the user's security record. SDD recommends OPB run and review the report annually to ensure that only authorized users have access to BAPS. This report will be available to security operators by July 31, 2017.

**Projected Completion Date:** 7/31/2017
**Contact Person/Phone:** Michael Jones / 850-717-9451

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 5:*** Certain security controls related to logging and monitoring of OPB network and application activities need improvement to ensure the confidentiality, integrity, and availability of OPB data and related IT resources.

***Recommendation:*** We recommend that OPB management enhance certain security controls related to logging and monitoring of OPB network and related application activities to ensure the confidentiality, integrity, and availability of OPB data and related IT resources.

**NOTE:** This finding was classified as CONFIDENTIAL. A more detailed finding and recommendation was provided to appropriate EOG management separate from the preliminary & tentative report. The response provided on this document should not contain detailed information that may expose security risks. However, any corrective actions taken will need to address the entirety of the risk(s) identified and only be reported as "Complete" once all actions have been taken.

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

## Management's Current Response

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

**Description of Corrective Action(s) or Explanation of No Action:**

Systems Design and Development (SDD) will make the required security enhancements related to the logging of OPB network and related application activities to ensure confidentiality, integrity and availability of OPB data and related IT resources.

**Projected Completion Date:** 12/29/2017
**Contact Person/Phone:** Michael Jones / 850-717-9451

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 6:*** As similarly noted in our report No. 2014-200, OPB records did not evidence independent review and testing of BAPS programming changes.

***Recommendation:*** We recommend that OPB management enhance configuration management controls to ensure that Team Foundation Server (TFS) records demonstrate that all BAPS programming changes are subject to independent review and testing.

**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:**

Team Foundation Server (TFS) is a robust development tool that provides the ability to maintain a flexible, secure development environment. SDD works in an environment where a TFS record is created for each upgrade or modification to the system. Each request has a parent record that contains information related to the requestor, programmer(s), tester and approver. Each task that is part of the development process will have a child record created to track program changes. Child records do not contain the detail information since that is contained within the parent record. SDD believes that this process provides the data required to ensure that changes are properly authorized, tested and approved; however, we recognize your concerns and recommendation and will continue to monitor these controls.

**Projected Completion Date:**
**Contact Person/Phone:** Michael Jones / 850-717-9451

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 7:*** EOG records did not always evidence that mobile device users had been appropriately authorized to access the EOG or OPB e-mail systems in accordance with EOG policies.

***Recommendation:*** We recommend that EOG management enhance mobile device authorization controls to ensure that, for all users of agency-owned and agency-managed mobile devices, EOG records evidence user agreement (UA) forms [are] approved in accordance with the Policy.

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

## Management's Current Response

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

**Description of Corrective Action(s) or Explanation of No Action:**

EOG IT staff will continue to obtain approvals for mobile device email access in accordance with EOG policies.

**Projected Completion Date:** 12/29/2017
**Contact Person/Phone:** Antony Zoghbi / 850-717-9276

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A

Corrective Action Plan in response to:
EOG Operational Audit - Information Security Controls & Mobile Device Mgmt. (May 30, 2017)

***Finding 8:*** Security controls over mobile device utilization need improvement to ensure the confidentiality, integrity, and availability of EOG and OPB data and related IT resources.

***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 related IT resources.

**NOTE:** This finding was classified as CONFIDENTIAL. A more detailed finding and recommendation was provided to appropriate EOG management separate from the preliminary & tentative report. The response provided on this document should not contain detailed information that may expose security risks. However, any corrective actions taken will need to address the entirety of the risk(s) identified and only be reported as "Complete" once all actions have been taken.

**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:**

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.

**Projected Completion Date:**
**Contact Person/Phone:** Antony Zoghbi / 850-717-9276

## Management's Previous Response

**Date of Response:** N/A

**Description of Corrective Action(s):** N/A

**Projected Completion Date:** N/A
**Contact Person/Phone:** N/A