RICK SCOTT
GOVERNOR

STATE OF FLORIDA

Office of the Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001

www.flgov.com
850-488-7146
850-487-0801 fax

January 30, 2018

The Honorable Rick Scott
Governor of the State of Florida
The Capitol, PL 05
Tallahassee, FL 32399

Dear Governor Scott:

In June 2017, the Auditor General released Report Number 2017-213, *Audit of Information Security Controls and Mobile Device Management*.

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

After six months, the results of our monitoring disclosed that corrective actions have been taken to address five of the eight report findings with corrective action still in progress to address three findings (see enclosed worksheets). Please note that this monitoring only involved Findings 2, 4, 5, and 7 from the original report. Findings 1, 3, 6, and 8 were previously addressed with corrective actions. We will conduct another monitoring on the remaining unresolved findings no later than December 2018.

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

Respectfully,

Eric W. Miller
Chief Inspector General

Enclosure

cc/enc: Jackie Schutz Zeckman, Chief of Staff
Diane Moulton, Director of Executive Staff
Dawn Hanson, Director of Administration
Alan Cash, Chief Information Officer, Information Systems
Cynthia Kelly, Director Office of Policy and Budget
Kathy DuBose, Coordinator Joint Legislative Auditing Committee

Executive Office of the Governor, Office of the Chief Inspector General
6-Month Follow-up to Chief Inspector General Report Number 2017-213
Audit of Information Security Controls and Mobile Device Management
Original Report Date: June 2017
Follow-up Date: January 30, 2018

Report Finding #2: Security Awareness Training

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

Report Recommendation:

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

Current Status of Management's Corrective Action: In Progress

Management's Response:

Training software has been purchased and is being set up for distribution to all EOG employees.

Projected Completion Date:

February 28, 2018

Primary Contact:

Alan Cash, Chief Information Officer
850-717-9200

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

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 (LAS/PBS) or Budget Amendment Processing System (BAPS) were conducted.

Report 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.

Current Status of Management's Corrective Action: In Progress

Management's Response:

Systems Design and Development (SDD) has modified server event logs to store when user accounts are deleted. These logs can then be searched to determine the date and time the action occurred.

Due to increased workload in the BAPS unit the security report detailing operator access has not yet been completed. Report is scheduled to be completed and deployed by the end of February 2018.

Projected Completion Date:
February 28, 2018

Primary Contact:
Michael Jones, Policy Coordinator
850-717-9451

Report Finding #5: Security Controls – Logging and Monitoring
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.

Report 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.

Current Status of Management's Corrective Action: Completed

Management's Response:
Systems Design and Development (SDD) has enhanced server logging to record certain security events. These logs are stored on the server and can be searched by network administrators.

Projected Completion Date:
January 2, 2018

Primary Contact:
Michael Jones, Policy Coordinator
850-717-9451

Report Finding #7: Security Awareness Training
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.

Executive Office of the Governor, Office of the Chief Inspector General
6-Month Follow-up to Chief Inspector General Report Number 2017-213
Audit of Information Security Controls and Mobile Device Management
Original Report Date: June 2017
Follow-up Date: January 30, 2018

Report 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.

Current Status of Management's Corrective Action: In Progress

Management's Response:

Device agreement forms are being signed by all approved mobile mail users and access to mail has been blocked to anyone not approved by management.

Projected Completion Date:

February 28, 2018

Primary Contact:

Alan Cash, Chief Information Officer
850-717-9200