From:	Atkins, Ronald
To:	Piepenbrink, Brad; Moulton, Diane; Hanson, Dawn; Cash, Alan; Kelly, Cynthia; JLAC
Cc:	Miller, Eric
Subject:	12-month Follow-up of Auditor General Audit #2017-213
Date:	Monday, July 09, 2018 2:59:17 PM
Attachments:	Final - Transmittal and memo.pdf

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 12 months, the results of our monitoring disclosed that corrective actions have been taken to address all of the eight report findings. Please note that this monitoring only involved Findings 2, 4, and 7 from the original report. Findings 1, 3, 5, 6, and 8 were previously addressed with corrective actions.

Please contact me if you have any questions about the follow-up review.

Thank you,

Ronnie Atkins, CPA, CIA, CMA, CIG
Director of Audits
Office of the Chief Inspector General
The Capitol
Tallahassee, FL 32399-0001
PH: 850.717.9255

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

July 9, 2018

JLAC Received
7/9/2018

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 12 months, the results of our monitoring disclosed that corrective actions have been taken to address all of the eight report findings. Please note that this monitoring only involved Findings 2, 4, and 7 from the original report. Findings 1, 3, 5, 6, and 8 were previously addressed with corrective actions.

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

Respectfully,

Eric W. Miller
Chief Inspector General

Enclosure

cc/enc: Brad Piepenbrink, Chief of Staff
Diane Moulton, Director of Executive Staff
Dawn Hanson, Director of Administration
Alan Cash, Chief Information Officer, Information Systems
Cynthia Kelly, State Budget Director
Kathy DuBose, Coordinator Joint Legislative Auditing Committee

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: Completed

Management's Response:
Security training software has been procured and implemented.

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: Completed

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.

BAPS report detailing user security was moved to production in February of 2018. OPB can run the report on demand to assess user access to the system.

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.

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: Completed

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.

Primary Contact:
Alan Cash, Chief Information Officer
850-717-9200