RICK SCOTT
GOVERNOR

JUSTIN M. SENIOR
SECRETARY

February 1, 2017

Mr. Justin M. Senior, Secretary
Agency for Health Care Administration
2727 Mahan Drive
Tallahassee, FL 32308

Dear Secretary Senior,

Enclosed is a six-month status report on the Auditor General's *Comprehensive Risk Assessments at Selected State Agencies*, Report Number 2017-004, issued August 1, 2016. This status report is issued in accordance with the statutory requirement to report on corrective actions resulting from the Auditor General's recommendations six months from the report date.

If you have any questions about this status report, please contact Mary Beth Sheffield at 412-3978.

Sincerely,

Eric W. Miller
Inspector General

EWM/szg
Enclosure: Six-Month Status Report of AG Report# 2017-004
cc/enc: Joint Legislative Auditing Committee
Melinda Miguel, Chief Inspector General, EOG
Scott Ward, Chief Information Officer, Information Technology

Agency for Health Care Administration
Auditor General Risk Assessments at Selected State Agencies (Report #2017-004)
Six-Month Status Report as of February 1, 2017

Finding 3:
Data Classification, Categorization of IT Systems, and Risk Mitigation. The risk assessment process for AHCA, DCF, DEO, DOE, and DOT did not include the classification of data and categorization of IT systems. Specifically, we found that the agencies':

- Specialized security awareness training was limited without the classification of data, including identification of confidential and exempt data that required specialized training.
- Audit logging and monitoring was limited without the identification of confidential and exempt data that requires logging and monitoring of access and transactions involving such data.
- Analysis of configuration management IT security controls for IT systems was ineffective without the classification of data and categorization of IT systems.
- Disaster recovery planning was less effective without the categorization of IT systems.
- IT security controls over backup resources were less effective without the identification of confidential and exempt data.
- Data loss prevention and incident response was limited without the identification of confidential and exempt data that should be monitored for loss or unauthorized access.
- Additionally, AHCA, DOE, and DOT did not developed risk mitigation plans for all IT security control deficiencies identified in the risk assessment process.

Recommendation:
To ensure effective, comprehensive risk assessments, we recommend that AHCA, DCF, DEO, DOE, and DOT management include the classification of data and categorization of IT systems in their risk assessment processes and that AHCA, DOE, and DOT management develop risk mitigation plans for all identified IT security control deficiencies.

Agency Response as of July 22, 2016:
AHCA will conduct an internal project within the agency to classify data. AHCA will also contract with a vendor to assist our agency in developing IT risk mitigation plans.

Agency Comments and Status of Finding as of February 1, 2017:
AHCA is continuing to plan for the data classification project. The contracted vendor has just completed (on 1/9/17) the legislatively assigned risk assessment so planning is underway. Enhanced confidential and exempt data training curriculum is underway for the Agency's "New Employee Orientation" and continuous "Keep Informed Training."

Agency Contact:
Karen Calhoun
(850) 412-4849

Finding 4:
IT Security Controls. Selected IT security controls for AHCA, DCF, DEO, DOE, and DOT need improvement to better ensure the confidentiality, integrity, and availability of agency data and IT resources.

Specifically, we found that:

- AHCA's policy on initial security awareness training needs improvement to ensure that the training is timely completed and acceptable use forms are signed by new employees prior to accessing IT resources, including confidential and exempt data.

- AHCA lacked a policy for configuration management addressing agency-managed hardware and software with the exception of mobile devices. Additionally, AHCA lacked a complete list of IT resource configurations.

- Certain IT security controls related to audit logging and monitoring and the use of administrative and service accounts need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising AHCA data and IT resources. However, we have notified appropriate AHCA management of the specific issues.

Recommendation:
To better ensure the confidentiality, integrity, and availability of agency data and IT resources, we recommend that AHCA, DCF, DEO, DOE, and DOT management improve their agencies' IT security controls.

Agency Response as of July 22, 2016:
AHCA is in the process of developing new security policies and procedures based on Rule 74-2, F.A.C., which became effective March 10, 2016. AHCA is also proposing a FY 2017-2018 Legislative Budget Request to address monitoring and audit logging solutions.

Agency Comments and Status of Finding as of February 1, 2017:
The Agency anticipates completion of information security policies and procedures by June 30, 2017. The Agency's LBR was submitted to the Legislature for consideration.

Agency Contact:
Karen Calhoun
(850) 412-4849