Office of Inspector General
4030 Esplanade Way, Suite 250
Tallahassee, FL 32399-0950
850-488-5285 | Fax: 850-921-3066

Ron DeSantis, Governor
Jonathan R. Satter, Secretary

September 4, 2020

Jonathan R. Satter, Secretary
Department of Management Services
4050 Esplanade Way
Tallahassee, Florida, 32399-0950

Re: **Auditor General Report No. 2020-170, State of Florida - Compliance and Internal Controls Over Financial Reporting and Federal Awards**

Dear Secretary Satter:

Section 20.055, Florida Statutes, requires the Inspector General to monitor the implementation of the agency's response to any report on the Department of Management Services (Department) issued by the Auditor General or by the Office of Program Policy Analysis and Government Accountability. The referenced statute further requires that the Inspector General provide a written response on the status of actions taken. The purpose of this letter is to provide updated information on the department's response to the Auditor General findings and fulfill these requirements.

In March 2020, the Auditor General released report No. 2020-170 titled *State of Florida Compliance and Internal Controls Over Financial Reporting and Federal Awards*. The report outlined 3 audit findings and recommendations regarding the Florida Agency for State Technology (FAST) which was transferred to DMS, effective July 1, 2019. Management is working to address the findings. The following pages detail the current progress of the Department to address the findings and recommendations.

If you have any questions, please let me know.

Sincerely,

Sarah Beth Hall
Inspector General

Enclosure

cc: Tami Fillyaw, Chief of Staff
    James Grant, State Chief Information Officer
    Andrew Richardson, Acting Deputy State Chief Information Officer
    Melinda Miguel, Chief Inspector General
    Kathy DuBose, Coordinator, Joint Legislative Auditing Committee

**Department of Management Services
Six-month Follow-up to the
Auditor General Report No. 2020-170**

Finding No. 2019-021: Appropriateness of Access Privileges

In our information technology (IT) operational audit report No. 2020-149, dated March 2020, we noted in Finding 5 that some access privileges did not promote an appropriate separation of duties or were not necessary based on users' assigned job responsibilities.

Recommendation: To promote compliance with State law and an appropriate separation of duties, we recommend that Department management properly restrict administrative access privileges to the mainframe, Windows servers, and Oracle database environments, and the interconnected network domains, to only those functions necessary for the user's assigned job responsibilities and ensure administrative accounts are timely disabled when no longer necessary.

Six-month Follow-up Response: The SDC initiated project number 2020-003 to address customer administrator access. The project involves generating agency-specific access listings from each platform, soliciting feedback on access from customer agencies, account clean-up, delegations of access, and where applicable, risk acceptance. The anticipated completion date is December 31, 2020.

Status Based on the Office of Inspector General Review: Open

Finding No. 2019-22: Security Controls – Logical Access, Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, Service Accounts, and Logging and Monitoring

In our information technology (IT) operational audit report No. 2020-149, dated March 2020, we noted in Finding 10 that certain State Data Center (SDC) security controls related to logical access, user authentication, and logging and monitoring, need improvement to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources.

Recommendation: We recommend that Department management improve certain security controls related to logical access, user authentication, and logging and monitoring to ensure the confidentiality, integrity, and availability of customer entity data and related IT resources.

Six-month Follow-up Response: The Department continues to evaluate and improve security controls to ensure the confidentiality, integrity and availability of data and IT resources. The anticipated completion date is July 21, 2021, and for logging and monitoring is December 31, 2022.

Status Based on the Office of Inspector General Review: Open

Finding No. 2019-023: Periodic Review of Access Privileges

In our information technology (IT) operational audit report No. 2020-149, dated March 2020, we noted in Finding 6 that SDC processes for performance and documentation of periodic access reviews need improvement to ensure assigned access remains appropriate.

Recommendation: We recommend that Department management perform comprehensive periodic reviews of logical and physical access privileges for users, maintain documentation of the reviews conducted, and ensure that access privileges are timely removed when no longer needed.

Six-month Follow-up Response: The SDC initiated project number 2020-003 to address customer administrator access. The project involves generating agency-specific access listings from each platform, soliciting feedback on access from customer agencies, account clean-up, delegations of access, and where applicable, risk acceptance. The anticipated completion date is December 31, 2020.

Status Based on the Office of Inspector General Review: Open