Department of
MANAGEMENT
SERVICES
We serve those who serve Florida

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. 2020-149, Department of Management Services State Data Center Operations Information Technology Operational Audit**

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 Information Technology Operational Audit report No. 2020-149 titled *Department of Management Services State Data Center (SDC) Operations*. The report outlined 10 audit findings and recommendations and management is working to address them. 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 BethHall

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. 2020-149

Finding No. 1: Disaster Recovery Planning

The SDC's disaster recovery plan (DRP), annual testing, and processes for customers subscribing to the SDC disaster recovery services need improvement to ensure that critical SDC operations are recovered and continue in the event of a disaster or other interruption in service.

Recommendation: To ensure recoverability of the critical applications maintained at the SDC in the event of a disaster or other interruption of service, we recommend that Department management:

- Conduct a BIA [Business Impact Analysis] to identify all critical SDC applications and include step-by-step instructions in the DRP for each identified critical application.
- Conduct testing of all identified critical applications, evaluate and timely remediate issues identified in testing, and incorporate necessary DRP modifications identified during the testing.
- Accurately define the roles and responsibilities for customer entities that subscribe to DR services and ensure testing requirements are documented with the customer entities prior to DR testing.
- Timely evaluate and remediate customer entity DR testing results.
- Ensure full-scale testing is performed to verify that all applications and infrastructure can be timely restored for customer entities subscribing to DR services.

Six-month Follow-up Response: The State Data Center (SDC) continues to work to refine and finalize updates to the Disaster Recovery (DR) plan. In addition to the build out of the Business Impact Analysis (BIA) information in the system, "CI Review Due" has been added to the customer portal. When a customer accesses the portal, they will see "CI Review Due" with a count of configuration items (CI's) that have not been reviewed in the past year. These updates to the Configuration Management Database (CMDB) are being discussed at the customer meetings to further ensure the information is being updated. On May 6, 2020 to May 7, 2020 a DST DR customers, all DR service subscriber agency DR test exercise occurred. Anticipated completion date is February 28, 2021.

Status Based on the Inspector General Review: Open

Finding No. 2: Continuity of Operations Planning (COOP)

The SDC's continuity of operations plan continues to need improvement to ensure the timely resumption of critical business operations in the event of a disaster or other interruption in service.

Recommendation: To promote the continued operations of the SDC, we recommend that Department management include in the SDC COOP, or incorporate by reference, all essential information specified in State law.

Six-month Follow-up Response: An updated version of the Essential Personnel – Emergency Management Duty procedure was completed July 20, 2020. Essential personnel were identified, notified of their designation, and the designation was documented in the employee action form. Additionally, an update of the Continuity of Operations Plan (COOP) was completed July 16, 2020 which includes requirements specified in State Law. The SDC will continue to refine requirements associated with the essential personnel designations and COOP.

Status Based on the Inspector General Review: Open

Finding No. 3: IT Asset Management

Inventory repositories for IT resources at the SDC were not complete and in some cases were not accurate, and configuration management database audits for servers were not performed, increasing the risk that IT resources may not be appropriately monitored, tested, and evaluated.

Recommendation: To ensure the accuracy of IT asset records, we recommend that Department management continue efforts to establish a complete, accurate, and up-to-date inventory of all SDC-managed hardware, perform annual reconciliations of the repository for physical assets to the data center cabinets, and complete the CMDB configuration audits annually.

Six-month Follow-up Response: Since the conclusion of the audit, the property management staff completed inventories of both data center floors. Additionally, the SDC continues to conduct CMDB configuration audits, 301 audits were conducted for fiscal year 2019-2020. Anticipated completion date is December 31, 2020.

Status Based on the Inspector General Review: Open

Finding No. 4: Backup Tape Reconciliations and Destruction

SDC processes for reconciling, tracking, and securing backup tapes need improvement to ensure that all backup tapes are accounted for and location and status records are accurate.

Recommendation: We recommend that Department management ensure that semiannual reconciliations of the backup systems that create backup tapes to the tracking system used to record the movement of tapes to the off-site storage location are performed as specified in Department procedures and documented. In addition, tape tracking system records should periodically be compared to the physical tape inventory at the off-site storage location. We also recommend that Department management ensure that tape location records are timely updated and accurate records of destruction are maintained.

Six-month Follow-up Response: Tape management staff are working daily to clean up tape track and ensure that tapes are processed correctly and documented. A tape reconciliation was completed in May 2020. Additionally, all tapes located at the off-site storage location were moved to the SDC for destruction. Destruction of these unneeded tapes is currently underway. Anticipated completion date is February 28, 2021.

Status Based on the Inspector General Review: Open

Finding No. 5: Appropriateness of Access Privileges

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. Anticipated completion date is December 31, 2020.

Status Based on the Inspector General Review: Open

Finding No. 6: Periodic Review of Access Privileges

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. Internal account review processes will continue to be evaluated and refined to ensure access is appropriate. Anticipated completion date is December 31, 2020.

Status Based on the Inspector General Review: Open

Finding No. 7: Backup Controls

SDC backup controls continue to need improvement to ensure backups for all IT resources requiring backup are appropriately performed and periodically tested for recoverability to ensure that customer data is readily recoverable in response to an unexpected event.

Recommendation: We recommend that Department management ensure that all required server backups are timely and successfully performed, legacy backup systems are monitored to help ensure backup tasks are timely and successfully completed, and backups are periodically tested for recoverability.

Six-month Follow-up Response: The SDC Backup and Recovery team continues to monitor backups to ensure they are timely and successful. Additionally, update of the Backup and Recovery Procedures was completed in February 2020. The procedures were updated to include all backup and corresponding monitoring process requirements. Anticipated completion date is December 31, 2020.

Status Based on the Inspector General Review: Open

Finding No. 8: Software Licensing

SDC procedures and processes for the management and monitoring of software licensing agreements need improvement to help prevent software licensing violations.

Recommendation: We recommend that Department management promptly complete the software asset management project and finalize procedures for managing and monitoring software licensing agreements.

Six-month Follow-up Response: Due to recent organizational changes, the SDC is working to identify proper placement of software asset management duties. Anticipated completion date is July 31, 2021.

Status Based on the Inspector General Review: Open

Finding No. 9: Performance Metrics

The SDC's monitoring and reporting of the performance metrics for database and network services provided to customer entities as defined in service-level agreements (SLAs) need improvement to ensure that critical incidents affecting the database and network services are timely detected, documented, and, as applicable, resolved and that performance uptime is accurately calculated and reported.

Recommendation: We recommend that Department management ensure that SDC database performance uptime metrics included in the SLAs are met, appropriate documentation for uptime performance statistics is maintained, and network services performance uptime metrics reflect all SDC-managed network devices used by each customer entity.

Six-month Follow-up Response: The SDC continues to evaluate and improve processes to ensure performance requirements are met and metrics are accurate. Anticipated completion date is December 31, 2020.

Status Based on the Inspector General Review: Open

Finding No. 10: Security Controls – Logical Access, Tape Encryption, Vulnerability Management, Configuration Management, User Authentication, Service Accounts, and Logging and Monitoring

Certain SDC security controls related to logical access, tape encryption, vulnerability management, configuration management, user authentication, service accounts, 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, tape encryption, vulnerability management, configuration management, user authentication, service accounts, 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. Anticipated completion date is July 1, 2021 except for logging and monitoring which is December 31, 2022.

Status Based on the Inspector General Review: Open