Department of
MANAGEMENT
SERVICES
We serve those who serve Florida

Office of Inspector General
4050 Esplanade Way, Suite 250
Tallahassee, FL 32399-0950
850-488-5285 | Fax: 850-921-3066

Ron DeSantis, Governor
Jonathan R. Satter, Secretary

January 17, 2020

Jonathan R. Satter, Secretary
Department of Management Services
4030 Esplanade Way
Tallahassee, Florida, 32399-0950

Re: **Auditor General Report No. 2019-220, Information Technology Operational Audit of DMS General Controls and Integrated Retirement Information System (IRIS)**

Dear Secretary Satter:

Section 20.055(6)(h), Florida Statutes, requires the Inspector General to monitor the implementation of the agency's response to any report on the Department of Management Services (DMS) 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 agency's response to the Auditor General findings and fulfill these requirements.

In June 2019, the Auditor General (AG) released its report No. 2019-220 titled Department of Management Services (Department) Information Technology (IT) General Controls and Integrated Retirement Information System (IRIS). The report outlined eight audit findings and nine recommendations for the Department. Management has addressed five of the eight findings and recommendations; therefore, these findings and recommendations are complete, pending verification by the Auditor General. The following pages detail the current progress of the Department to address the findings and recommendations.

If you have any questions, please call me at 413-8740.

Sincerely,

Sarah Beth Hall

Sarah Beth Hall
Inspector General

Enclosure

cc: Tammy Fillyaw, Chief of Staff
David DiSalvo, Director of Division of Retirement
Shirley Beauford, Assistant Director of Division of Retirement
Bob Ward, 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 #: 2019-220

Finding No. 1: Timely Disabled IRIS User Accounts

The Division of Retirement (Division) did not timely disable the IRIS access privileges of some former employees.

Recommendation:

We recommend that Division management ensure that IRIS user accounts are timely disabled upon a user's separation from Department employment.

Six-month Follow-up Response:

The current security procedures state that IRIS access must be deactivated within 1 day of termination. The solution involves Active Directory account management which is currently undergoing an ownership transition to the Department's Office of Information Technology (OIT). The Division anticipates completing the remediation for this finding in partnership with OIT after the completion of the Departmental domain merge scheduled to complete by end of FY 19/20.

Status Based on the Inspector General Review: Partially Complete

Finding No. 2: Access Authorization Documentation

IRIS access privileges granted for some users did not match the access roles authorized.

Recommendation:

We recommend that Division management improve controls to ensure that the IRIS access privileges granted are authorized as documented on the ENFs.

Six-month Follow-up Response:

Some users did not have an Employee Notification Form (ENF) that documented authorization to use IRIS 2.0 screens. The team received emailed instructions on 5/30/19 that clarified that they should specify the appropriate role for IRIS whenever an ENF is done for any reason. The new training material (implemented September 2019) contained this same information.

A new ENF (for IRIS access authorization only) was completed for each person authorized to use IRIS. This reauthorization project was completed July 5, 2019. The procedures were updated to clarify that

Supervisors and Data Owners should specify the appropriate role for IRIS whenever an ENF is done for any reason. The updates were completed September 2019.

Status: Complete, pending verification by Auditor General

Finding No. 3: Appropriateness of Access Privileges

The access privileges for two IRIS security administrators did not promote an appropriate separation of duties and were not restricted to their assigned job duties. Similar findings were noted in prior audits of the Department, most recently in our report No. 2018-077.

Recommendation:

We recommend that Division management limit user access privileges to IRIS and related IT resources and restrict users to only those access privileges necessary for the users' assigned job duties and that promote an appropriate separation of duties.

Six-month Follow-up Response:

The Department has completed the necessary changes to further restrict access to IRIS production libraries and to promote a separation of duties for the IRIS security administrators.

Status: Complete, pending verification by Auditor General

Finding No. 4: Periodic Review of Privileged Accounts

Department and Division management need to establish procedures for conducting periodic reviews of privileged accounts used to manage the Department's network domain and the Division's network domain and high-risk network devices.

Recommendation:

We recommend that Department management establish and implement procedures for conducting comprehensive periodic reviews of privileged accounts used to manage the Department's network domain and retain documentation of the reviews conducted. We also recommend that Division management establish and implement procedures for conducting comprehensive periodic reviews of privileged accounts used to manage the Division's network domain and high-risk network devices and retain documentation of the reviews conducted.

Six-month Follow-up Response:

The Department developed and implemented procedures to audit and document privileged account

access as outlined in the recommendation. The Division implemented the Department's developed procedures of auditing and documenting privileged account access.

Status: Complete, pending verification by Auditor General

Finding No. 5: IT Security Policies and Procedures

The Department had not established IT security policies and procedures to protect and manage Department and Division IT boundaries.

Recommendation:

We recommend that Department management establish, implement, and maintain IT security policies and procedures to manage the protection of Department data and IT resources.

Six-month Follow-up Response:

The Department has remediated the finding by implementing a manual process to request and approve elevated access.

Interim Solution: Manual process for requesting and approving elevated access:

An email approval for elevated access (privileged accounts) will be required by one level of supervisor higher than the direct supervisor or the System Owner. This email approval must be attached to the ticket requesting the access. For contractors, the email approval will come from the Contract Manager.

Additionally, the Department will develop a Plan of Action and Milestones (POAM) to evaluate implementation of an approval processing system for account elevation access requests to include policies and procedures as outlined in the recommendation.

Plan of Action: Implement a system for requesting and approving elevated access:

The Department intends to provide a POAM solution via building a request and approval process using Cherwell, the service management system planned for deployment throughout DMS with assistance from the Cherwell subject matter experts in the DMS Division of State Technology.

Status: Complete, pending verification by Auditor General

Finding No. 6: Change Management Controls

Division change management controls for IRIS program changes need improvement to ensure that program changes are appropriately authorized and approved for implementation into the production environment.

Recommendation:

We recommend that Division management improve IRIS program change management procedures to ensure that all program changes moved into the production environment are appropriately authorized and approved for implementation.

Six-month Follow-up Response:

Management has taken actions directly related to finding. The Department is in the process of implementing an enhanced Software Investigation Report change management process to include additional approval steps.

Status: Partially Complete

Finding No. 7: Backup Controls

Department backup policies and procedures need improvement to define the frequency of recoverability testing of Division-managed backups.

Recommendation:

We recommend that Department management establish policies and procedures and related controls that define the frequency of recoverability testing of Division-managed backups and retain evidence of the testing conducted.

Six-month Follow-up Response:

Response actions taken and completed, no additional actions needed. The Department developed a procedure that defines the frequency of recoverability testing for Division of Retirement managed backups and developed a process for retaining documentation of the recoverability tests.

Status: Complete, pending verification by Auditor General

Finding No. 8: Security Controls – Logical Access, User Authentication, Configuration Management, and Logging and Monitoring

Certain security controls related to logical access, user authentication, configuration management, and logging and monitoring need improvement to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

Recommendation:

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

Six-month Follow-up Response:

Department management is working to improve certain security controls related to logical access, user authentication, configuration management, and logging and monitoring to ensure the confidentiality, integrity, and availability of Department data and related IT resources.

Status: Partially Complete