STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-220
June 2019

DEPARTMENT OF MANAGEMENT SERVICES

Information Technology General Controls and Integrated Retirement Information System (IRIS)

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Management Services

The Department of Management Services is established by Section 20.22(1), Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, the following individuals served as Department Secretary:

Jonathan Satter	From February 5, 2019 [a]
Erin Rock	Through January 8, 2019

[a] Position vacant from January 9, 2019, through February 4, 2019

The team leader was Wayne Revell, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

DEPARTMENT OF MANAGEMENT SERVICES

Information Technology General Controls and Integrated Retirement Information System

SUMMARY

This operational audit of the Department of Management Services (Department) focused on evaluating Department information technology (IT) general controls and selected IT application controls applicable to the Integrated Retirement Information System (IRIS). The audit also included follow-up on the finding noted in our report No. 2018-077. Our audit disclosed the following:

Finding 1: The Division of Retirement (Division) did not timely disable the IRIS access privileges of some former employees.

Finding 2: IRIS access privileges granted for some users did not match the access roles authorized.

Finding 3: 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.

Finding 4: 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.

Finding 5: The Department had not established IT security policies and procedures to protect and manage Department and Division IT boundaries.

Finding 6: 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.

Finding 7: Department backup policies and procedures need improvement to define the frequency of recoverability testing of Division-managed backups.

Finding 8: 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.

BACKGROUND

The Department of Management Services (Department) is responsible for managing various business- and workforce-related functions. Business operations consist of State purchasing, real estate development and management, telecommunications, fleet management, and private prison monitoring. Workforce operations include human resource management, State group insurance, and retirement.

The Division of Retirement (Division) was created within the Department by Section 121.1905, Florida Statutes. The Department, along with the Division, uses the Integrated Retirement Information System (IRIS) to support the Department's business processes related to the Florida Retirement System (FRS).

The business processes supported by IRIS include member enrollment and the maintenance of member information, receipt of contributions from FRS participating employers, tracking of members' employer and employee contributions and service histories, calculation of retirement benefits, and the issuance of the retiree payroll file processed by the Department of Financial Services. The FRS Online application is an extension of IRIS and uses Internet technology to provide information and services to members, employers, and retirees.

Application and database administration support for IRIS and the FRS Online application, as well as support for the Division's day-to-day information technology (IT) needs, were outsourced by the Department to Deloitte Consulting Limited Liability Partnership (Deloitte). Deloitte is responsible for providing the Division's IT functions, which include network and application security administration, application programming, and database administration functions.

FINDINGS AND RECOMMENDATIONS

Finding 1: Timely Disabled IRIS User Accounts

Agency for State Technology (AST) rules[1] require agency control measures that ensure IT access is removed when an IT resource is no longer required. Prompt action to disable access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent the misuse of the access privileges.

During the period July 1, 2018, through November 27, 2018, 31 employees assigned to the Division separated from Department employment. To determine whether these 31 former employees' IRIS user accounts were timely disabled we requested the accounts' disabled dates. Division management indicated that records of disabled dates for IRIS user accounts were not retained prior to October 5, 2018, at which time the Division implemented additional logging capabilities to record when an IRIS user account is disabled. Accordingly, we examined the available records of IRIS user accounts disabled during the period October 5, 2018, through February 18, 2019, and the active IRIS user accounts as of November 28, 2018, to determine whether the 31 former employees' IRIS user accounts had been timely disabled when the employees separated from Department employment and, if not, if the accounts were still active. We found that, as of November 28, 2018, active IRIS user accounts did not exist for the 31 former employees and the accounts for 3 of the former employees had been timely disabled. However, we also found that:

- IRIS user accounts for 2 of the former employees were not timely disabled and remained active for 4 and 6 days after their separation dates. In response to audit inquiry, Division management indicated that, although the user accounts were not timely disabled, the IRIS user access privileges for the former employees were not used subsequent to their employment separation dates.
- Department records did not evidence the user account disabled dates for the remaining 26 former employees; therefore, the Department could not demonstrate that the IRIS user accounts were timely disabled.

[1] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

Timely disabling IRIS user accounts upon an employee's separation from Department employment reduces the risk that the IRIS access privileges may be misused by the former employee or others.

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

Finding 2: Access Authorization Documentation

AST rules[2] provide that agency information owners are responsible for establishing and authorizing the types of privileges and access rights appropriate to system users. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges authorized by management. Additionally, appropriately maintained access authorization documentation facilitates the complete and accurate assignment of user access privileges. The Division utilizes Employee Notification Forms (ENFs) for IRIS access actions, including IRIS access authorizations and deactivations.

As part of our audit, we requested for our examination access authorization documentation for 25 of the 170 users with active access privileges to IRIS as of November 28, 2018, to determine whether the IRIS access privileges granted were appropriately authorized and documented. The access authorization documentation requested consisted of ENFs showing the IRIS platform requested, access roles authorized, and supervisory approval. Our audit procedures disclosed that the access roles granted to 7 of the 25 IRIS users did not match the access roles authorized on the users' corresponding ENF.

Assigning access that is not explicitly authorized limits the Division's ability to demonstrate and ensure that user access privileges granted to users are authorized by management and are appropriate for the accomplishment of the users' assigned job duties.

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

Finding 3: Appropriateness of Access Privileges

Effective access controls include measures that limit users' access privileges to only those system functions necessary to perform their assigned job duties and promote an appropriate separation of duties. AST rules[3] require each agency to ensure that access permissions are managed, incorporating the principles of least privilege and separation of duties.

Our audit procedures disclosed that some users had inappropriate access privileges to IRIS and related IT resources. Our evaluation of the access privileges assigned to the two IRIS security administrators as of November 30, 2018, disclosed that the two IRIS security administrators were each assigned an account that provides full update access privileges to IRIS production libraries, contrary to the users' assigned job duties and an appropriate separation of duties.

[2] AST Rule 74-2.003(5)(g)6., Florida Administrative Code.

[3] AST Rule 74-2.003(1)(d), Florida Administrative Code.

Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. 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.

Finding 4: Periodic Review of Privileged Accounts

AST rules[4] require agency information owners to review access rights (privileges) periodically based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. An effective periodic review consists of identifying the current access privileges of all system users and evaluating the assigned access privileges to ensure that they align with the users' job responsibilities.

Our audit procedures disclosed that the Department had not established procedures for comprehensive periodic reviews of privileged accounts used to manage the Department's network domain and the Division's network domain and high-risk network devices. Although comprehensive periodic review procedures had not been established, Department management, or Division management where applicable, indicated that periodic reviews of privileged accounts:

- Within the Department's network domain were performed quarterly.
- Within the Division's network domain were performed every other month.
- Used to manage the Division's high-risk network devices were periodically performed.

However, a defined process to conduct and document the reviews did not exist and Department or Division records evidencing the reviews conducted during the period July 1, 2018, through November 5, 2018, were not maintained.

Procedures for comprehensive periodic reviews of privileged accounts used to manage the Department's network domain and the Division's network domain and high-risk network devices that require the identification of the users assigned the privileged accounts, an evaluation of the users' necessity for the privileged accounts, and documentation of the appropriateness of the privileged account assignments, increase management's assurance that the assignment of the privileged accounts to users is authorized and remains appropriate.

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.

[4] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

Finding 5: IT Security Policies and Procedures

Security policy is management's directives to create a security program, establish its goals, and assign responsibilities. Procedures are detailed steps to be followed to accomplish particular security-related tasks. Effective IT security controls include documented, management-approved policies and procedures that describe the information security management program for providing security for the information and information systems that support the operations and assets of the agency. AST rules[5] require each agency to ensure that security policies and procedures are maintained and used to manage the protection of information systems and assets.

Our audit procedures disclosed that policies and procedures had not been established for the assignment of privileged accounts for the Division's high-risk network devices, the Department's network domain, and the Division's network domain. Established policies and procedures for protecting and managing access privileges help prevent inappropriate access, thereby reducing the risk that Department data and IT resources may be compromised.

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.

Finding 6: Change Management Controls

Effective change management controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation into the production environment. For example, to ensure that only approved program changes are implemented, program changes should be reviewed for appropriateness before the changes are moved into the production environment. Division procedures require a technical peer review for completed program changes that documents approval prior to implementing the program changes into the production environment.

As part of our audit procedures, we selected 12 of the 29 program changes made to IRIS during the period July 1, 2018, through October 30, 2018, to evaluate the appropriateness of the program change management controls. Our audit disclosed that IRIS program change management controls need improvement. Specifically, we found that Division records did not evidence that 4 of the 12 selected program changes were properly authorized by the Division or that 3 of the 12 program changes were properly approved by the Division for implementation into the production environment.

The absence of appropriate program change management controls increases the risk that program changes may not be implemented in a manner consistent with management's expectations.

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.

[5] AST Rule 74-2.003(5), Florida Administrative Code.

Finding 7: Backup Controls

Effective backup controls include policies and procedures that provide guidance for an entity's backup processes, including identification of the IT resources requiring back up, the frequency of backups, and the periodic testing for recoverability to prevent or minimize the damage to automated operations that can occur from unexpected events. AST rules[6] require each agency to develop procedures to prevent loss of data and to ensure that backups of information are conducted, maintained, and tested.

Our audit procedures disclosed that Division backup controls for IRIS resources need improvement. Specifically, the Department had not established policies and procedures to define the frequency of recoverability testing of Division-managed backups. Additionally, while Division management stated that Division-managed backups were periodically tested to ensure recoverability, the Division was unable to provide documentation to evidence such testing.

The lack of policies and procedures that define the frequency of recoverability testing of Division-managed backups and require documentation evidencing the conduct and results of such testing limits management's assurance of recoverability in the event of a loss of IRIS production data.

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.

Finding 8: Security Controls – Logical Access, User Authentication, Configuration Management, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to logical access, user authentication, configuration management, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate management of the specific issues.

Without adequate security controls related to logical access, user authentication, configuration management, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of Department data and related IT resources may be compromised.

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.

PRIOR AUDIT FOLLOW-UP

As noted in Finding 3, the Department partially corrected the finding included in our report No. 2018-077.

[6] AST Rules 74-2.003(5)(d) and 74-2.006(1)(c), Florida Administrative Code.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from September 2018 through March 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected business process application controls related to IRIS data input, processing, and output during the period July 2018 through February 2019 and selected actions thereto. The audit also focused on evaluating selected application-level and other IT general controls over logical access, user identification and authentication, logging and monitoring, change management, and configuration management. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, the deficiency disclosed in our report No. 2018-077.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel and reviewed Department and Division documentation to obtain an understanding of:
  - IRIS background information including the purpose or goals involving financial, operations, and compliance requirements.
  - The data and business process flows in IRIS for the calculation of retirement benefits and to identify and document key sources of data input, key application transactions and processes, and key types of application data output.
  - The IRIS computing platform including applicable hardware, software, operating system, and security software for the IRIS application and database.
  - Logical access, authentication, and configuration management related to the administration of the IT infrastructure for the high-risk network devices and the IRIS application and database servers.
  - Management and operational processes for background screening for staff employed in positions with sensitive IT responsibilities and access privileges (i.e., positions of special trust).
  - Logical access controls for privileged network accounts used in the administration of IRIS, application change control process, and backup processes for IRIS application and database servers.
- Evaluated IRIS application access controls. Specifically, we:
  - Examined Division records to determine whether data owners and section supervisors performed periodic reviews of IRIS access privileges to ensure continued appropriateness for each user.
  - Determined whether IRIS update access roles were appropriately authorized for 25 of the 170 IRIS users as of November 28, 2018.
  - Evaluated the appropriateness of IRIS update access privileges for 25 of the 170 IRIS users as of November 28, 2018.
  - Determined whether IRIS user accounts were timely disabled for employees who separated from Department employment during the period July 1, 2018, through November 27, 2018.
- Evaluated the appropriateness of IRIS application and database identification and authentication controls.
- Evaluated access controls for IRIS database administration accounts. Specifically, we:
  - Evaluated Division procedures for assigning IRIS database administration user accounts.
  - Examined Division records for the 2 user accounts assigned to IRIS database administrators as of December 5, 2018, and the 11 Team Foundation Server user accounts assigned to

application programmers as of November 29, 2018, to determine whether the user accounts were necessary and appropriately restricted to promote an appropriate separation of duties.

  - Evaluated Division procedures and examined Division records to determine whether periodic reviews were performed to evaluate the appropriateness of IRIS database administrator accounts.

- Evaluated logging and monitoring controls related to security changes made to the IRIS application and changes made directly to the IRIS database. Specifically, we:
  - Evaluated Division procedures and examined Division records to determine whether periodic reviews were performed of IRIS application and database security events.
  - Evaluated various IRIS change and tracking reports that demonstrate the logging of IRIS security permission changes.
- Evaluated patch management processes for operating system software and database software for the IRIS application and database servers. Specifically, we:
  - Evaluated Division policies and procedures for application and database server patch management.
  - Determined the timeliness of patch management for 10 of the 41 servers supporting the IRIS application and database management as of October 2018.
  - Determined the timeliness of patch management for the four production servers hosting the IRIS databases as of November 20, 2018.
  - Determined the timeliness of software updates to the server supporting the IRIS production database for the production server hosting the database management software as of November 21, 2018.
- Evaluated Division procedures and configuration management controls and examined Division records for the Division's high-risk network devices as of November 14, 2018, to determine the timeliness of updates to the high-risk network devices.
- Evaluated Division logical access controls and user authentication controls for technical user accounts with elevated privileges (administrative accounts) associated with high-risk network devices, including security logging and the periodic review of access. Specifically, we:
  - Examined Division records to determine whether policies and procedures were available and adequate for defining the assignment of administrative access privileges for high-risk network devices.
  - Evaluated the access privileges to the Division's three high-risk network devices as of November 14, 2018, and determined the appropriateness of the assigned access.
  - Examined Division records to assess the sufficiency of procedures for the performance of periodic reviews of administrative access privileges for the high-risk network devices.
  - Evaluated authentication controls for the Division's three high-risk network devices.
  - Evaluated whether audit and accountability policies and procedures were sufficient for identifying high-risk network device security events.
  - Evaluated the logging, review, analysis, reporting, and investigating of inappropriate and unusual activity related to high-risk network devices.
- Evaluated controls for background screenings for employees and contractors in positions of special trust. Specifically, we:
  - Examined Department records to assess the sufficiency of policies and procedures requiring background screening for positions of special trust (Level 2 screenings).

- Determined whether appropriate background screenings were timely performed as of November 28, 2018, for 30 of the 204 Division employees and contracted consultants in positions of special trust.

- Evaluated logical access and authentication controls for privileged network accounts, including periodic reviews of access. Specifically, we:
  - Evaluated the sufficiency of policies and procedures defining the assignment of privileged network accounts.
  - Evaluated the effectiveness of logical access controls as of November 9, 2018, for the Department's privileged network accounts on the Department's domain.
  - Evaluated the effectiveness of logical access controls as of November 9, 2018, for the Division's privileged network accounts on the Division's domain.
  - Examined Department and Division records to assess whether procedures for the periodic review of the appropriateness of access to the Department and Division's network domains were adequate.
- Evaluated authentication controls for the Department's and Division's network domains.
- Evaluated access controls for IRIS technical user application accounts (programmers and security administrators). Specifically, we:
  - Examined Division records to determine whether procedures defining the assignment of IRIS programmer and security administrator privileges had been established and were sufficient.
  - Evaluated the appropriateness of access privileges for the two security administrators to the IRIS application (end-user access) as of November 28, 2018, and to production libraries as of November 30, 2018, to ensure assigned access privileges were necessary and an appropriate separation of duties was maintained.
  - Evaluated whether an appropriate separation of duties as of November 29, 2018, was maintained for the nine IRIS programmers and two users with deployment access to the IRIS production environment.
- Evaluated change management controls for the authorization, testing, approval, and implementation to production for IRIS program changes. Specifically, we:
  - Examined Division records to determine whether policies and procedures for the IRIS program change process had been established and were sufficient.
  - Examined Division records supporting 12 of the 29 IRIS program changes implemented into the production environment during the period July 1, 2018, through October 30, 2018.
- Evaluated data storage, backup, and recovery controls, including policies and procedures for data storage methods and locations and backup processes for the IRIS application and database servers. Specifically, we evaluated the backups for 10 of the 44 IRIS application and database servers as of November 12, 2018, to determine the adequacy of periodic backups.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT of management SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
Tel: 850-488-2786 | Fax: 850-922-6149

Ron DeSantis, Governor

Jonathan R. Satter, Secretary

June 21, 2019

Ms. Sherrill F. Norman, CPA
Auditor General
Suite G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Pursuant to subsection 11.45(4)(d), Florida Statutes, this is our response to your report, ***IT Operational Audit of the Department of Management Services, Information Technology General Controls and Integrated Retirement Information System (IRIS).*** Our responses correspond with the findings and recommendations related to the Department of Management Services contained in the preliminary and tentative finding report.

If further information is needed concerning our response, please contact Sarah Beth Hall, Inspector General, at 488-5285.

Sincerely,

Jonathan R. Satter
Secretary

JRS/sk-a

Enclosure

cc: David Clark, Chief of Staff
Tami Fillyaw, Deputy Secretary of Workforce Operations
Bob Ward, Chief Information Officer
David Disalvo, Director of Retirement
Melinda M. Miguel, Chief Inspector General
Sarah Beth Hall, Inspector General

Auditor General's 2019 IT Operational Audit of DMS,

IT General Controls and Integrated Retirement Information System (IRIS)

Responses to Preliminary and Tentative Findings

Finding 1
Timely Disabled IRIS User Accounts

Finding: We found that, as of November 28, 2018, active IRIS user accounts did not exist for the 31 former employees and the accounts for 3 of the former employees had been timely disabled. However, we also found that:

- IRIS user accounts for 2 of the former employees were not timely disabled and remained active for 4 and 6 days after their separation dates. In response to audit inquiry, Division management indicated that, although the user accounts were not timely disabled, the IRIS user access privileges for the former employees were not used subsequent to their employment separation dates.
- Department records did not evidence the user account disabled dates for the remaining 26 former employees; therefore, the Department could not demonstrate that the IRIS user accounts were timely disabled.

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

Responsible Area: Division of Retirement

Contact Person: David DiSalvo, Division Director
(850) 487-4133
David.Disalvo@dms.myflorida.com

Management Response:
The Department concurs with the findings and the recommendation. Regarding bullet 1, the Department will continue to provide its IRIS access security training and information to appropriate division staff to ensure that IRIS user accounts are timely (within 24 hours) disabled upon a user's separation from Department employment. Regarding bullet 2, a remediation of this finding was implemented on October 5, 2018 when the Division implemented additional logging capabilities to record when an IRIS user account is disabled. The Department expects to provide additional information about IRIS security to division staff by September 30, 2019.

Finding 2
Access Authorization Documentation

Finding: Our audit procedures disclosed that the access roles granted to 7 of the 25 IRIS users did not match the access roles authorized on the users' corresponding ENF.

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

Responsible Area: Division of Retirement

Contact Person: David DiSalvo, Division Director
(850) 487-4133
David.Disalvo@dms.myflorida.com

Management Response:
The Department concurs with the finding and the recommendation. The Department will develop a plan of action to ensure current IRIS user access matches the access privileges authorized as documented on the ENFs. The Department expects to have the plan conceptualized and documented by September 30, 2019.

Finding 3
Appropriateness of Access Privileges

Finding: Our audit procedures disclosed that some users had inappropriate access privileges to IRIS and related IT resources. Our evaluation of the access privileges assigned to the two IRIS security administrators as of November 30, 2018, disclosed that the two IRIS security administrators were each assigned an account that provides full update access privileges to IRIS production libraries, contrary to the users' assigned job duties and an appropriate separation of 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.

Responsible Area: Division of Retirement

Contact Person: David DiSalvo, Division Director
(850) 487-4133
David.Disalvo@dms.myflorida.com

Management Response:
The Department concurs with the finding and recommendation. The Department has completed the necessary changes to further restrict access to IRIS production libraries.

Finding 4
Periodic Review of Privileged Accounts

Finding: Our audit procedures disclosed that the Department had not established procedures for comprehensive periodic reviews of privileged accounts used to manage the Department's network domain and the Division's network domain and high-risk network devices. Although comprehensive periodic review procedures had not been established, Department management, or Division management where applicable, indicated that periodic reviews of privileged accounts:

- Within the Department's network domain were performed quarterly.
- Within the Division's network domain were performed every other month.
- Used to manage the Division's high-risk network devices were periodically performed.

However, a defined process to conduct and document the reviews did not exist and Department or Division records evidencing the reviews conducted during the period July 1, 2018, through November 5, 2018, were not maintained.

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.

Responsible Area: Office of Information Technology

Contact Person: Bob Ward, Chief Information Officer
(850) 413-9169
Bob.Ward@dms.myflorida.com

Management Response:
The Department concurs with the findings and recommendations. The Department will develop a procedure to audit and document privileged account access as outlined in the recommendation. The Department expects to have the procedure complete and implemented by September 30, 2019. The Division will implement the Department's developed procedures of auditing and documenting privileged account access at that time.

Finding 5
IT Security Policies and Procedures

Finding: Our audit procedures disclosed that policies and procedures had not been established for the assignment of privileged accounts for the Division's high-risk network devices, the Department's network domain, and the Division's network domain.

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.

Responsible Area: Office of Information Technology

Contact Person: Bob Ward, Chief Information Officer
(850) 413-9169
Bob.Ward@dms.myflorida.com

Management Response:
The Department concurs with the finding and recommendation. The Department has remediated the finding by implementing a manual process to request and approve elevated access. Additionally, the Department will develop a plan of action to evaluate implementation of an approval processing system for account elevation access requests to include policies and procedures as outlined in the recommendation. The Department expects to have the plan completed by September 30, 2019.

Finding 6
Change Management Controls

Finding: Our audit disclosed that IRIS program change management controls need improvement. Specifically, we found that Division records did not evidence that 4 of the 12 selected program changes were properly authorized by the Division or that 3 of the 12 program changes were properly approved by the Division 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.

Responsible Area: Division of Retirement
Contact Person: David DiSalvo, Division Director
(850) 487-4133
David.Disalvo@dms.myflorida.com

Management Response:
The Department concurs with the finding and recommendation. The Department has updated its change management controls by eliminating Technical Support Center (TSC) System Investigation Requests (SIRs). In addition, the Department is in the process evaluating and enhancing the SIR process to include additional approval steps. The Department expects to have the plan finalized by September 30, 2019 and begin implementation shortly afterward.

Finding 7
Backup Controls

Finding: Our audit procedures disclosed that Division backup controls for IRIS resources need improvement. Specifically, the Department had not established policies and procedures to define the frequency of recoverability testing of Division-managed backups. Additionally, while Division management stated that Division-managed backups were periodically tested to ensure recoverability, the Division was unable to provide documentation to evidence such testing.

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.

Responsible Area: Office of Technology

Contact Person: Bob Ward, Chief Information Officer
(850) 413-9169
Bob.Ward@dms.myflorida.com

Management Response:
The Department concurs with the finding and recommendation. The Department will develop a procedure that defines the frequency of recoverability testing for Division of Retirement managed backups and develop a process for retaining documentation of the recoverability tests. The Department expects to have the procedure finalized and implemented by September 30, 2019.

Finding 8
Security Controls – Logical Access, User Authentication, Configuration Management, and Logging and Monitoring

Finding: Our audit procedures disclosed that certain security controls related to logical access, user authentication, configuration management, and logging and monitoring need improvement.

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.

Responsible Area: Office of Information Technology

Contact Person: Bob Ward, Chief Information Officer
(850) 413-9169
Bob.Ward@dms.myflorida.com

Management Response:
The Department concurs with the finding and recommendation. The estimated completion date for corrective actions is September 30, 2019.