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

Rick Scott, Governor

Erin Rock, Secretary

July 24, 2017

Erin Rock, Secretary
Florida Department of Management Services
4050 Esplanade Way, Suite 285B
Tallahassee, FL 32399

Dear Secretary Rock:

In accordance with section 20.055, Florida Statutes, the enclosed documents represent our explanation of the six-month status of the findings and recommendations included in the Auditor General published Report No. 2017-101, ***Integrated Retirement Information System (IRIS) – Technology Operational Audit.***

The findings and recommendations appear in the same order as they appeared in the report.

If further information is needed concerning the status, please do not hesitate to contact me.

Sincerely,

Dawn E. Case
Inspector General

DEC/yvl

Enclosure

cc: Elizabeth Stevens, Director of Division of Retirement
Shirley Beauford, Assistant Director of Division of Retirement
David Zeckman, Chief of Staff
Heather Best, Senior Director of Executive Operations
Eric Miller, Chief Inspector General
Sherill F. Norman, Auditor General
Joint Legislative Auditing Committee

Audit Findings Status Update Form

Status Date	**Report/Agency #**	**Report Title/Agency Name**
7/24/17	2017-101	IT Operational audit of IRIS

Contact Person	**Title**	**Phone No.**	**Email Address**
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com

Activity	**Accountability**	**Schedule**	
Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement	Yes	**2/28/17**

Finding		**Access Authorization Documentation**
No.	**1**	
Date	**1/24/17**	

Finding	Complete and accurate IRIS access authorization documentation was not maintained, thereby limiting management's assurance that IRIS user access privileges were authorized and appropriately assigned.
Recommendation	We recommend that Department management improve controls to ensure that properly completed and approved access authorization forms are retained.
Management/Agency Response	In response to the finding in the prior audit, the Division revised the ENF to require supervisors to select the specific IRIS access role that was being authorized and made the field required. The Security Guidelines Manual was updated to reflect the new requirement and supervisors were advised of changes. This repeat finding resulted from previous changes being implemented prospectively. Of the accounts identified from the sample as having an issue related to the access authorization form, all but one had access that predated the changes enacted by the Division as a result of the prior audit. The last account was updated and documented by the bureau chief in the six- month review process. The Division will complete an overall review of our IRIS access authorization process. This includes requests for access, changes, and deactivations as well as the six-month review for appropriate access levels. Upon the completion of this project, the Security Guidelines Manual will be revised, and staff will be trained. Additionally, after we complete our process review and update our procedures, the Division will document the IRIS access authorizations for all persons that currently have IRIS access. The Division expects to complete this review and document authorizations by February 28, 2017.

[redacted]

Status Update-6 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG X Closed	The division completed an overall review and updated the Microsoft Word version of the Employee Notification Form (ENF) on February 28, 2017, to reflect that the "IRIS Data Owner (Chief/Manager)" authorizes IRIS access. The division designated IRIS Data Owners (Bureau Chiefs, Assistant Director, and Director) and as of March 1, 2017, ENFs are sent to the IRIS security administrator by the IRIS Data Owner instead of the immediate supervisor as was done previously. The division is currently working with DMS IT staff on the implementation of an ENF accessible directly via Sharepoint workflow with IRIS data owner access authorization built in which will automate portions of the ENF process. In addition, the division updated the Security Guidelines manual and trained staff on the new ENF procedures and the importance of properly documenting IRIS access in February and March 2017. The Division also reauthorized all IRIS user access on February 24, 2017.
Status Update-12 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG □ Closed	
Status Update-18 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG □ Closed	

Audit Findings Status Update Form

Status Date	**Report/Agency #**	**Report Title/Agency Name**	
7/24/17	2017-101	IT Operational audit of IRIS	
Contact Person	**Title**	**Phone No.**	**Email Address**
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com
Activity	**Accountability**	**Schedule**	
Application Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement	No	**1/6/17**

Finding		
No.	2	**Appropriateness of Access Privileges**
Date	1/24/17	

Finding	The access privileges for some IRIS users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for their assigned job duties.
Recommendation	We recommend that Department management limit user access privileges to IRIS data and IT resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.
Management/Agency Response	IRIS Application Users: The Division determined that the employees noted in the audit did not have a need to update the Contributions Rate Table for their assigned job duties and removed this access on October 7, 2016. Employees can only view the contributions rate information. The new process for updating the Contributions Rate Table is for appropriate management staff to send a change request with the spreadsheet of the updated rates to the IT help desk. Requests are logged and assigned a work number. Once the new rate information is updated to the IRIS table, the manager or the designated employee will review the rate information for accuracy. The manager will notify the help desk to close the ticket after verifying that the rate information is correct. The Division will complete a review of reference tables containing critical FRS information to determine whether employee access to edit the reference table is appropriate. If edit capability is not appropriate, the access will be removed. Security Administrators: The Division removed the database administrator function from the Security Administrators on 10/10/16 which restricts their access to the IRIS production database and prevents updates to the IRIS change log. In addition, the Division will make changes to the semi-annual PowerLock review process that will no longer require security administrators to have production end user update access to IRIS to generate IRIS role reports. Application Programmers: The Division removed the update privileges on the change log table from the programmer's account. Also, the Division has implemented a process to export and archive the IRIS change logs each time an IRIS change occurs, preserving the record as files in an archive folder with a timestamp on each file. Also, implemented are access restrictions that prevent the logs from being deleted or changed by application programmers and database administrators. Database Administrators: The Division implemented a process to export and archive the IRIS change logs each time an IRIS change occurs which preserves a record in an archive folder with a timestamp on each file. Also, implemented are access restrictions that prevent the logs from being deleted or changed by application programmers and database administrators.
[redacted]	
Status Update-6 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG X Closed	The changes included in the Department's response to this finding have been implemented. **A. IRIS Application Users:** The Division removed update access to the contribution rate information for all employees. Employees can only view the contributions rate information. The new process for updating the Contributions Rate Table is for appropriate management staff to send a change request with the spreadsheet of the updated rates to the IT help desk. Requests are logged and assigned a work number. Once the new rate information is updated to the IRIS table, the manager or the designated employee will review the rate information for accuracy. The manager will notify the help desk to close the ticket after verifying that the rate information is correct. The Division completed a review of reference tables containing critical FRS information to determine whether employee access to edit the reference table is appropriate. Based on the review, appropriate action was taken. **B. Security Administrators:** The Division removed the database administrator function from the Security Administrators, which restricts their access to the IRIS production database and prevents updates to the IRIS change log. In addition, the Division developed an automated role report that eliminated the need for security administrators to have production end user update access to IRIS to generate IRIS role reports. C. **Application Programmers:** The Division removed the update privileges on the change log table from the programmer's account. Also, the Division has implemented a process to export and archive the IRIS change logs each time an IRIS change occurs, preserving the record as files in an archive folder with a timestamp on each file. Also, the Division implemented access restrictions that prevent the logs from being deleted or changed by application programmers and database administrators. D. **Database Administrators:** The Division implemented a process to export and archive the IRIS change logs each time an IRIS change occurs which preserves a record in an archive folder with a timestamp on each file. Also, implemented are access restrictions that prevent the logs from being deleted or changed by application programmers and database administrators.
Status Update-12 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	
Status Update-18 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	

Audit Findings Status Update Form

Status Date	**Report/Agency #**	**Report Title/Agency Name**		
7/24/17	2017-101	IT Operational audit of IRIS		
Contact Person	**Title**	**Phone No.**	**Email Address**	
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com	
Activity	**Accountability**	**Schedule**		
Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**	
	Division of Retirement	No	2/28/17	

Finding		**Deactivation of Access Privileges**
No.	3	
Date	1/24/17	
Finding		The Department did not have procedures for timely deactivating IRIS accounts for users who no longer required access and did not timely deactivate the IRIS accounts for some users.
Recommendation		We recommend that Department management establish procedures that specify when a user's access privileges should be deactivated and take appropriate action to ensure that IRIS accounts are timely deactivated when a user separates employment or access to the information is no longer required.
Management/Agency Response		The Division is currently reviewing the IRIS access authorization process. One focus of the review is ensuring timely deactivations. The Security Guidelines manual will be updated with additional information for deactivating IRIS users who no longer need access to perform their job duties. Additionally, for terminated employees, the Division has implemented another control procedure to review the report of active IRIS accounts within one business day of a person's termination date to verify that the terminated employee is not listed with an active IRIS account. The Division expects to complete the review of the IRIS access authorization process by February 28, 2017.

[redacted]

Status Update-6 months ☐ Open ☐ Management/Agency Assumes Risk ☒ Partially Complete ☐ Complete Pending Verification by OIG Closed	As stated in Finding 1, the Security Guidelines Manual was updated and the Division created new IRIS procedures. Training was provided to all supervisors regarding the importance of properly documenting changes to IRIS access. As of February 28, 2017, Administrative Services is responsible for reviewing Employee Notification Forms for terminated employees to ensure IRIS access has been removed by the next business day. This is accomplished by running the real-time "Powerlock User List" from IRIS to determine whether the employee is still in the IRIS database. If the employee's name and IRIS role code are no longer listed, the employee has been removed. If the employee's name and IRIS role code are still listed the employee has not been removed. In this instance, Administrative Services will contact IT services immediately to follow up on the request for termination on the ENF.
Status Update-12 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	
Status Update-18 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name
7/24/17	2017-101	IT Operational audit of IRIS

Contact Person	Title	Phone No.	Email Address
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com

Activity	Accountability	Schedule	
	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
Security	Division of Retirement	No	2/28/17

Finding		
No.	4	Periodic Review of User Access Privileges
Date	1/24/17	

Finding	Department procedures did not ensure the timely and effective review of the appropriateness of user access privileges granted to IRIS.
Recommendation	We recommend that Department management improve controls and enhance Department procedures addressing the conduct of periodic reviews of IRIS access privileges. Such enhancements should require the use of system-generated lists of users and a specified time frame within which Bureau Chiefs must complete their review. Department management should also ensure that the reviews are performed every 6 months as required by Department procedures.
Management/Agency Response	The Division will create a new system generated report listing each user's IRIS access level for the scheduled six-month IRIS access review. The Division will update the six-month review procedures to include time frames for starting and completing all reviews. Staff will be trained on the updated procedures. The six-month review process is included in the overall access authorization process project that the Division expects to complete by February 28, 2017.

[redacted]

Status Update-6 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG X Closed	The Division developed procedures regarding the periodic reviews which include specific timeframes for beginning and completing the reviews as well as procedures surrounding how issues identified in the review are documented and remediated. The Division also created a new system generated report listing each user's IRIS access level for the scheduled quarterly IRIS access review. Staff was trained on the new procedures in February and March 2017 . Using the new procedures and system generated report, the IRIS Security Administrator provided all IRIS Data Owners with their IRIS User Access Role Report for review in February and April, 2017 and all certification forms were returned timely to the Assistant Director following review and all identified issues were timely remediated.
Status Update-12 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG □ Closed	
Status Update-18 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG □ Closed	

Audit Findings Status Update Form

Status Date	**Report/Agency #**	**Report Title/Agency Name**	
7/24/17	2017-101	IT Operational audit of IRIS	
Contact Person	**Title**	**Phone No.**	**Email Address**
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com
Activity	**Accountability**	**Schedule**	
Security	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Division of Retirement	**No**	**1/9/17**

Finding		**Service Accounts**
No.	**5**	
Date	**1/24/17**	

Finding	Some service accounts inappropriately allowed interactive log-on increasing the risk that the confidentially, integrity, and availability of Department data and IT resources may be compromised.
Recommendation	We recommend that Department management improve controls to ensure that the capability for interactive log-on for service accounts is appropriately restricted.
Management/Agency Response	The Division has implemented a database log-on trigger to only allow database service account authentication from trusted server sessions.

[redacted]

Status Update-6 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG ☒ Closed	The changes included in the Department's response for this finding have been implemented. The Division implemented a database log-on trigger to only allow database service account authentication from trusted server sessions.
Status Update-12 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG □ Closed	
Status Update-18 months □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIG □ Closed	

Audit Findings Status Update Form

Status Date	Report/Agency #	Report Title/Agency Name
7/24/17	2017-101	IT Operational audit of IRIS

Contact Person	Title	Phone No.	Email Address
Elizabeth Stevens	Division Director	(850) 778-4400	Elizabeth.Stevens@dms.myflorida.com

Activity	Accountability	Schedule	
Security	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
	Division of Retirement	Yes	2/28/17

Finding		
No.	6	Security Controls – User Authentication and Monitoring
Date	1/24/17	

Finding	Certain security controls related to user authentication and monitoring for IRIS-related IT resources need improvement to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.
Recommendation	We recommend that Department management improve certain security controls related to user authentication and monitoring for IRIS-related IT resources to ensure the confidentiality, integrity, and availability of IRIS data and related IT resources.
Management/Agency Response	While the Division made changes to remediate this finding following the prior audit, the Division supports the recommendation and has implemented measures to enhance security controls related to user authentication and monitoring of IRIS related IT resources. The AG reports these conditions in a separate confidential document. In order to prevent compromising the confidentiality of the document, the Division has not responded directly to the recommendation.

[redacted]

Status Update-6 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☒ Complete Pending Verification by OIG ☐ Closed	The changes included in the Department's response for this finding have been implemented. The Division implemented measures to enhance security controls related to user authentication and monitoring of IRIS related IT resources.
Status Update-12 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	
Status Update-12 months ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIG ☐ Closed	