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

Chad Poppell, Secretary

March 16, 2016

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

Dear Secretary Poppell:

In accordance with section 20.055, Florida Statutes, the attached documents represent our explanation of the six-month status of the findings and recommendations included in the AG published Report No. 2016-018, ***IT Operational Audit of the Division of Retirement Integrated Retirement Information System (IRIS).***

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

If further information is needed concerning our response, please do not hesitate to contact me.

Sincerely,

Walter Sachs
Inspector General

WS/sk-a

Enclosure

cc: Darren Brooks, Deputy Secretary, Workforce Operations
Dan Drake, Director of Retirement
Elizabeth Stevens, Assistant Director of Retirement
Yolanda Lockett, Audit Director
Melinda Miguel, Chief Inspector General
Sherrill F. Norman, Auditor General
Joint Legislative Auditing Committee

Audit Status Report Update Form

Status Date	Report No	Report Title
3/11/2016	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Application Security	IT	Yes	8/31/2015

Finding	
No.	1
Date	9/3/2015

Appropriateness of Access Privileges

Finding	Four IRIS database accounts continued to be assigned access privileges that should be granted only to database admininstrators
Recommendation	Department management should require Deloitte management to improve access controls to ensure that system privileges are appropriately granted only to database administrators.
Response/Action Plan	The Division believes it fully complied with the previous report by taking steps to eliminate or limit the use of these accounts and modifying the access privileges without adversely impacting operations based on the prior audit. However, the Division supports the current recommendation and has implemented additional measures. The Division has either locked or adjusted the access privileges of these accounts. In addition, the Division will enhance its monthly review of database access privileges to verify that only database administrators and approved system accounts have the appropriate access privilege granted. The enhanced monthly review process will be implemented by August 31, 2015.
Status Update-6mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☑ Complete	The changes included in the Department's response for this finding have been implemented.
Status Update-12mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	
Status Update-18mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	

Audit Status Report Update Form

Status Date	Report No.	Report Title
3/11/2016	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Security	IT	Yes	9/30/2015

Finding		
No.	2	Generic Database Accounts
Date	9/3/2015	
Finding		Some generic database accounts continued to be active and were not expired or locked.
Recommendation		Department management should require Deloitte management to ensure that all generic database accounts are expired or locked.
Response/Action Plan		The Division believes it fully complied with the previous report by taking steps to either discontinue the use of or implement logging on the accounts needed to manage objects. However, the Division supports the recommendation that additional measures can be implemented. In addition to the logging, the Division will make changes to the deployment processes for both developers and DBAs to enable deployments from DBA accounts. This will allow for locking generic database accounts. The Division will also enhance its monthly review of access privileges by reviewing all active database accounts that are not IRIS end-user accounts to ensure that generic accounts are expired or locked. These processes will be implemented by September 30, 2015.

Status Update-6mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☑ Complete pending verification by OIG ☐ Complete	The changes included in the Department's response for this finding have been implemented.
Status Update-12mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	
Status Update-18mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	

Audit Status Report Update Form

Status Date	Report No.	Report Title
3/10/2016	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Security		No	9/3/2015

Finding	
No.	3
Date	9/3/2015

Access Authorization Documentation

Finding	Access privileges granted to IRIS were not always appropriately authorized and documented.
Recommendation	Department management should ensure that all access privileges granted to IRIS are appropriately documented as authorized by management and that such documentation specifies the IRIS roles.
Response/Action Plan	All persons with IRIS access have the appropriate IRIS access. However, the Divison of Retirement concurs with this finding in that the authorization of appropriate access was not always properly documented. The Division and has verified current processes and implemented process changes to ensure that access privileges granted to IRIS are appropriately documented as authorized by management and that such documentation specifies the IRIS role code. The recently revised Security Guidelines Manual (rev. July 2015), includes the policy and procedure for updating user access privileges in IRIS. As noted in the audit findings and recommendations, Division management notified the IT Operations and Maintenance (O & M) vendor (Deloitte), on June 15, 2015 that no changes, additions or deletions to IRIS privileges should be made without the proper authorization documentation. This document is internally referred to and titled the Employee Notification Form. This is a multi-purpose form that documents and initiates employee related actions such as; new hires, terminations, promotions, location information, assigned equipment and resources, network access requests, building access and other information. Subsequent to the notification to the IT O & M vendor, the Employee Notification form was updated to include drop-down boxes to provide the role codes for managers to select from when initiating role code changes, additions or deletions in IRIS for their staff. A NA (not applicable), check box was also added to be used if a particular employee action does not require an IRIS role code change. In addition to this, a listing of all of the Role Codes and Definitions and a listing of Role Codes by Position were provided to division managers and supervisors. In order to provide an additional level of review of assigned role codes and ensure role codes are current and appropriate, the Employee Database was modified to include information for assigned role codes for each position. Monthly reports will be run from the Employee Database and matched against the IRIS system information to verify that staff have appropriate role codes assigned in IRIS. Any discrepancies will be resolved on a monthly basis.
Status Update-6mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☑ Complete	The changes included in the Department's response for this finding have been implemented.
Status Update-12mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	
Status Update-18mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete	

Audit Status Report Update Form

Status Date	Report No.	Report Title
3/11/2016	Preliminary & Tentative	Information Technology Operational Audit of IRIS

Contact Person	Program/Process	Phone No.
Elizabeth Stevens	Retirement	(850) 778-4400

Activity	Accountability	Schedule	
	Responsible Unit	Repeat Finding	Anticipated Completion Date
Security	IT	Partially	9/3/2015

Finding		
No.	4	Security Controls -- User Authentication and Logging
Date	9/3/2015	
Finding		Certain security controls related to IRIS database user authentication and logging for IRIS-related IT resources needed improvement.
Recommendation		Department management should improve certain security controls related to user authentication and logging for IRIS-related IT resources to ensure the continued confidentiality, integrity, and availability of IRIS data and IRIS-related IT resources.
Response/Action Plan		The Division believes it fully complied with the previous report by taking steps to improve user authentication controls based on the prior audit. However, the Division supports the current recommendation and will implement additional measures to further improve these security controls. In addition, the Division agrees to improve its logging procedures related to IRIS. 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.
Status Update-6mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☑ Complete pending verification by OIG ☐ Complete		The changes included in the Department's response for this finding have been implemented.
Status Update-12mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete		
Status Update-18mo ☐ Open ☐ Management assumes risk ☐ Partially Complete ☐ Complete pending verification by OIG ☐ Complete		