RICK SCOTT
Governor

DEPARTMENT OF MANAGEMENT
SERVICES

CRAIG J. NICHOLS
Agency Secretary

MEMORANDUM

DATE: May 21, 2013

TO: Craig Nichols, Secretary

FROM: Walter Sachs, Inspector General

SUBJECT: **Six-Month Follow-up to Auditor General Report No. 2013-042**

In accordance with Chapter 20.055, Florida Statutes, the following is our explanation of the six-month status of findings and recommendations included in the Auditor General's Report No. 2013-042, ***Integrated Retirement Information System (IRIS) – Information Technology Operational Audit.*** Our response addresses the findings and recommendations in the same order as they appear in the report.

This report contained one confidential finding. There is no requirement that the Department provide responses to confidential findings contained in Auditor General reports. However, as a matter of practice, the Office of Inspector General requires program areas to provide responses to confidential findings to ensure that action is being taken to implement the recommendations. Accordingly, a separate attachment regarding Finding 4 is enclosed for your review only.

Six-Month Status Report

Finding No. 1: Access Privileges

The IRIS application and database access privileges of some employees, contractors, and automated processes exceeded what was necessary to accomplish their job responsibilities or functions. Also, procedures for authorization documentation and review of access privileges to IRIS and the IRIS database needed improvement.

Recommendation:

The Department should require Deloitte to enhance its periodic review of existing access privileges, remove the inappropriate access privileges to the IRIS application and database, and maintain appropriate documentation of management authorizations of Deloitte IT staff access privileges.

Office of Inspector General
4050 Esplanade Way | Suite 217 | Tallahassee, Florida 32399-0950 | Tel: 850.488.5285 | Fax: 850.921.3066
www.dms.MyFlorida.com

RECEIVED
MAY 23 2013

Response:

IRIS Application

The Division of Retirement concurs with this recommendation. Starting with the next scheduled semi-annual review of user access privileges in February 2013, all users with active IRIS power lock accounts will be included in the report. Due to complications associated with maintaining users with secondary IRIS accounts, the division has adopted a policy of no longer allowing users to have more than one IRIS account.

In addition, the division will enhance its semi-annual review process by including in the report a list of additional access privileges assigned to IRIS roles. This tracking sheet will be dispersed in subsequent semi-annual reviews. This new process will go into effect during the next scheduled semi-annual review in February 2013.

IRIS Database

The Division of Retirement concurs with this recommendation. The division will enhance its periodic review of existing access privileges so in addition to ensuring that IRIS database access is restricted to active Deloitte IT staff and department employees, Deloitte will run database queries monthly to list specific inappropriate database access privileges so they can be removed.

The division will implement a procedure to maintain appropriate documentation of Deloitte IT staff access privileges, including the list of staff with database administration functions. This will be implemented by January 31, 2013.

Current Status of Recommendation:

IRIS Application
As of February 2013, the secondary accounts have been eliminated thereby including only users with active IRIS power lock accounts. On March 4, 2013 division management implemented a procedure to review role/menu changes that govern user access privileges.

IRIS Database
Procedures for maintaining appropriate documentation has been implemented and is accessible on the division network. Authorization for access privileges was given to Deloitte on January 25, 2013.

Office of Inspector General Position:

We agree with the actions taken by the Division of Retirement and recommend this finding be closed.

Finding No. 2: User Identification

Generic user identification codes (IDs) for database administration and the movement of programs into the production environment were being shared by Deloitte Consulting LLP (Deloitte) IT staff.

Recommendation:

The Department should require Deloitte to assign a unique user ID to each person within the Deloitte IT staff who is authorized to perform IT functions for IRIS.

Response:

The Division of Retirement concurs with this recommendation. The division will assign unique database user ID's to each member of the Deloitte IT staff and they will use those ID's for database access, moving programs to production, and other database administration functions to the extent possible. This will be implemented by March 31, 2013.

Current Status of Recommendation

The creation of unique IDs for development staff was completed February 2013. Deloitte staff members are using the newly created IDs for accessing the production database.

Office of Inspector General Position:

We agree with the actions taken by the Division of Retirement and recommend this finding be closed.

Finding No. 3: Timely Deactivation of IRIS Application Access Privileges

The Department did not timely deactivate the IRIS access privileges of two former employees.

Recommendation:

The Department should ensure that the IRIS application access privileges of former employees are timely deactivated to minimize the risk of compromising IRIS data and IT resources.

Response:

The Division of Retirement concurs with this recommendation. The division employs a practice requiring supervisors to complete an internal form referred to as the "Employee

Notification form" whenever an employee terminates. This practice generally works in a very satisfactory manner notifying IT and Administrative Services sections of terminated employees. This sets into motion a wide range of activities, including removing security access to IRIS and the division's physical facilities. More emphasis will be placed on supervisors adhering to the requirement that they complete the necessary forms when employees terminate. An additional review process of active IRIS accounts has been put into place to help catch any terminated employees or non-employees missed by this work process. This new monthly review process became effective on July 1, 2012.

Current Status of Recommendation

This recommendation was implemented on July 1, 2012, prior to completion of the audit.

Office of Inspector General Position:

We agree with the actions taken by the Division of Retirement and recommend this finding be closed.

Finding No. 5: Program Change Management

Some IRIS application program change controls needed improvement.

Recommendation:

The Department should document written program change control procedures and enforce effective program change controls that provide for an appropriate separation of duties and the identification of the individuals performing the tasks. In addition, the Department should also review its approval documentation practices to ensure that all intended program changes, once completed, are reviewed and moved into the production environment upon approval.

Response:

The Division of Retirement concurs with this recommendation. The division will implement additional change control procedures and enhance the System Investigation Request Form (SIR) Tracking System to enforce better program change controls that provide for appropriate separation of duties, reviews, and identification of individuals performing the tasks.

A Final SIR Review process has been put in place where application team leads review all the SIRs closed each month to verify that design documentation for the SIR is complete, test scripts are complete, test execution date and tester name are entered, peer reviews are complete, release notes are complete, code is moved to production, and SIR production date is stamped.

The SIR Tracking system has been enhanced so Release Notes are captured with better detail and cover Retirement Online (ROL) objects, report objects, and database structure changes with controls on the persons able to process each type of object. The system will ensure that the person moving each change to production is different from the person entering the release note for the program object. This will be implemented by March 31, 2013, so all SIRs completed subsequent to March 31, 2013, will use the enhanced SIR Tracking system.

Current Status of Recommendation

The configuration management plan that governs the SIR Review Process was updated in March 2013. The SIR Tracking System has been enhanced so that more detail is captured for release notes to cover Retirement Online (ROL) objects, report objects, and database structure changes with controls on the persons able to process each type of object.

Office of Inspector General Position:

We agree with the actions taken by the Division of Retirement and recommend this finding be closed.

WS/ls

Attachment

cc: David W. Martin, CPA, Auditor General
Kathy Dubose, Coordinator, Joint Legislative Audit Committee
Erin Rock, Chief of Staff
Darren Brooks, Deputy Secretary
Dan Drake, Retirement Director
Elizabeth Stevens, Assistant Director
Marlene Williams, Legislative Affairs