REPORT NO. 2013-042
NOVEMBER 2012

DEPARTMENT OF MANAGEMENT SERVICES

DIVISION OF RETIREMENT
INTEGRATED RETIREMENT INFORMATION SYSTEM (IRIS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

DEPARTMENT OF MANAGEMENT SERVICES

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

Craig J. Nichols	From July 9, 2012
Scott Stewart	Interim, From April 1, 2012, to July 9, 2012
John P. 'Jack' Miles	From January 26, 2011, to March 31, 2012

The audit team leader was Art Wahl, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CITP, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF MANAGEMENT SERVICES

Division of Retirement

Integrated Retirement Information System (IRIS)

SUMMARY

Section 121.1905, Florida Statutes, created the Division of Retirement (Division) within the Department of Management Services (Department). The Division administers the Florida Retirement System (FRS) and also has oversight responsibility for the Firefighter and Municipal Police Pension Plans authorized by Chapters 175 and 185, Florida Statutes, respectively. The Integrated Retirement Information System (IRIS) is used by the Division to support the functions required to provide retirement services.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to IRIS. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2009-200, relating to Department IT controls over IRIS.

The results of our audit are summarized below:

SECURITY CONTROLS

Finding No. 1: 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.

Finding No. 2: 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.

Finding No. 3: The Department did not timely deactivate the IRIS access privileges of two former employees.

Finding No. 4: Certain security controls related to user authentication needed improvement.

PROGRAM CHANGE CONTROLS

Finding No. 5: Some IRIS application program change controls needed improvement.

BACKGROUND

The Department uses IRIS to support the Department's business processes relating to the retirement life cycle of FRS-covered employees. The business processes supported by IRIS include the enrollment and maintenance of members in the system, tracking of members' employer contributions and service histories throughout their careers, calculation of retirement benefits, and the issuance of the retiree payroll file that is processed by the Department of Financial Services. IRIS is also used to process and maintain FRS Investment Plan payrolls and data. The Retirement Online application is an extension of IRIS that uses Internet technology to provide information and services to members, employers, and retirees.

IRIS and Retirement Online application support, as well as the Division's day-to-day information technology needs, were outsourced to Deloitte by the Department. 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

Security Controls

Finding No. 1: Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job duties and document the access privileges that have been authorized. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction. Periodic review of user access privileges helps ensure that access privileges remain appropriate. Our evaluation of selected IRIS application and database access controls disclosed the need for improved Department management of access privileges. These conditions, described in the following paragraphs, increased the risk of unauthorized disclosure, modification, or destruction of IRIS data and IT resources.

IRIS Application

The Department had procedures for a semiannual review of user access privileges to the IRIS application. Reports of IRIS application users and their assigned access privileges were distributed to the respective Bureau Chiefs for review. The Bureau Chiefs reviewed these reports to identify needed changes to access privileges. However, these reports were limited to access privileges that were linked to active network accounts. As a result, access privileges for 14 IRIS users that were not linked to active network accounts were excluded from the Bureau Chiefs' reviews.

Our audit disclosed that the access privileges for 8 of the 14 IRIS users were not required by the users to perform their assigned job duties and access for the remaining 6 users fully or partially duplicated access granted through other IRIS access accounts that were linked to active network accounts. Although IRIS access privileges that were not linked to active network accounts could not be used, the access could be inadvertently granted upon the reactivation or creation of an associated network account.

We also noted that an additional 10 IRIS users were assigned update access privileges that were not necessary for their current job duties. The unnecessary update access privileges were further indicative of the need for enhanced Department review of IRIS application access privileges.

IRIS Database

Deloitte's policy was to periodically review access privileges to the IRIS database but this review was limited to ensuring that access was restricted to active Deloitte IT staff and Department employees and did not include an evaluation of the appropriateness of this access. Our audit tests of selected IRIS database access privileges disclosed that 9 user IDs associated with Deloitte IT staff and computer processes were granted access privileges in excess of what was necessary for the staff's job duties or for the functions of the computer processes. Of the 9 user IDs, 7 had the ability to grant their access privileges to other user IDs and 5 of the user IDs had system privileges, such as creating tables and users and altering database attributes, that were normally granted only to database administrators. Of the 9 user IDs, 2 were used by Deloitte IT staff and the remaining user IDs were used by computer processes. Deloitte did not maintain documentation of management access authorizations for Deloitte IT staff who had access to perform database administration functions.

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.

Finding No. 2: User Identification

The effectiveness of access controls is dependent, in part, on the ability to uniquely identify system users. Unique identification of individual users assists in the assignment of access privileges and provides a mechanism for establishing responsibility for system actions.

Deloitte IT staff used four generic user IDs to access the IRIS database. Two of the four generic user IDs were among the user IDs previously identified in Finding No. 1 as having access privileges in excess of what was necessary for the Deloitte IT staff's job duties. In addition, Deloitte IT staff used a generic user ID to move IRIS application programs into the production environment. Without the ability to uniquely identify Deloitte IT staff performing database administration functions and moving programs into the production environment, the Department's ability to establish responsibility for these actions may be limited. In addition, allowing Deloitte IT staff to utilize generic user IDs increases the risk that staff may gain unnecessary access privileges.

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.

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

Effective IT access controls include provisions for the timely deactivation of former employee and contractor access privileges to ensure that the access privileges are not misused by the former employee, contractor, or others. For the 13 Department employees and 4 Deloitte IT staff who terminated employment or contractual services between July 1, 2011, and March 30, 2012, we reviewed IRIS application access privileges to determine whether the former employee and contractor access privileges had been deactivated in a timely manner. Our review disclosed that the access privileges of 2 of the 13 former Department employees had not been deactivated in a timely manner. Specifically, the 2 former Department employees retained inquiry and limited update access privileges to IRIS for three and six days beyond their termination dates. The access privileges of the 2 former Department employees were not used subsequent to the dates of their employment terminations. Nevertheless, without the timely deactivation of former Department employee access privileges to IRIS, the risk was increased that the access privileges may be misused by the former employees or others.

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.

Finding No. 4: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to user authentication that needed 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 Department management of the specific issues. Without

adequate security controls related to user authentication, the risk is increased that the confidentiality, integrity, and availability of Department data and IT resources may be compromised.

Recommendation: The Department should improve user authentication controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Program Change Controls

Finding No. 5: Program Change Management

Effective controls over modification of application programs help ensure that only authorized, tested, and approved changes are implemented. The effectiveness of program change controls is enhanced when management's expectations for the control of program changes are documented in the form of written procedures.

IRIS application program changes were made and moved into the production environment by Deloitte IT staff. Procedures had been developed and implemented to record programming change requests including the authorization, testing, approval, documentation, and movement of completed programming changes into the production environment. However, our audit disclosed that some IRIS application program change controls needed improvement.

We evaluated a sample of 26 of 53 *System Investigation Request Forms* (*SIRs*) from July 1, 2011, through March 15, 2012, that included 23 program change requests and 3 requests involving action other than changes to programs. For 1 of the 23 program change requests included in our sample, no documentation was available indicating that the program change was tested and by whom. Also, for 3 of the program change requests included in our sample, no documentation was available indicating who had moved the updated program code into the production environment. Under these conditions, the risk was increased that unauthorized program changes could be moved into the production environment.

In addition, the updated program code for 1 of the 23 program change requests had been overlooked by Deloitte IT staff and had not been moved into the production environment. This program change was intended to correct data reporting for actuarial analysis. Although the program change had been coded and approved, it was inadvertently not moved into the production environment in a timely enough manner for the intended corrections to be applied to the data reported as of June 30, 2011. Manual adjustments were required to reverse the errors caused by the uncorrected programming errors. In response to audit inquiry, Department staff indicated that this program change had since been moved into the production environment prior to reporting the June 30, 2012, data.

Completed program changes for the Retirement Online application were moved into the production environment by Deloitte programming staff. A procedure had been implemented for a Deloitte programmer who was not responsible for the programming changes to move the programs into the production environment. However, this procedure had not been established in writing. Although our audit did not disclose any instances where Deloitte programming staff moved their own program changes into production, the lack of a written procedure increases the risk that the same programmer may both modify and implement Retirement Online application programs, increasing the risk of unauthorized system changes.

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.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for all findings included in our report No. 2009-200.

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 March 2012 through June 2012 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to IRIS 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. An additional objective was to determine the extent to which the Department had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2009-200.

The scope of our audit focused on evaluating selected IT controls applicable to IRIS, including selected general IT controls over system modification, operating system patch management, logical access to programs and data, disaster recovery planning, and selected application IT controls and user controls relevant to IRIS. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from July 2011 through June 2012.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of IRIS, including the database, network, server, operating system, and user environments; the workflow of data entry for updating historical earnings and contribution data; and input of selected data through file transfer.
- Obtained an understanding of selected general, application, and user controls, including policies, procedures, hardware, software, organizational structure, and personnel relating to IRIS.
- Evaluated on a sample basis the effectiveness of the IRIS program change management process. Specifically, we reviewed a sample of 26 of 53 *SIRs* to determine whether changes were authorized, tested, approved, documented, and appropriately moved into production.
- Tested the appropriateness of logical access privileges to IRIS programs. Specifically, we evaluated the appropriateness of access privileges for moving updated programs into the production environment.

- Evaluated on a sample basis the effectiveness of procedures for authorizing and granting access to IRIS. Specifically, we reviewed a sample of 20 of 185 IRIS user IDs as of March 28, 2012, to determine whether the access to IRIS was authorized and appropriate based on assigned job duties.
- Tested the effectiveness of procedures for disabling the IRIS user access privileges of former Department employees and Deloitte IT staff who had terminated employment or contractual services.
- Observed and evaluated the effectiveness of selected logical access controls and password settings in ensuring that administrative access privileges to the Department's network, application, and servers were appropriately restricted and enforced an appropriate separation of duties.
- Tested the effectiveness of selected logical access controls and password controls for database administration functions.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated November 15, 2012, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

RICK SCOTT
Governor

DEPARTMENT OF MANAGEMENT
SERVICES

CRAIG J. NICHOLS
Agency Secretary

4050 Esplanade Way | Tallahassee, Florida 32399-0950 | Tel: 850.488.2786 | Fax: 850.922.6149

November 15, 2012

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your report, Department of Management Services Integrated Retirement Information System. Our response corresponds with the order of the preliminary and tentative findings and recommendations contained in the draft report.

If further information is needed concerning our response, please contact John Davis, Audit Director, at 488-5285.

Sincerely,

Craig J. Nichols
Agency Secretary

Attachment

cc: Darren Brooks, Deputy Secretary
Erin Rock, Chief of Staff
Kristen Beach, Director of Communications
Stephanie Leeds, Director of Legislative Affairs
Sarabeth Snuggs, Director of Retirement

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin, CPA
Page 2
November 15, 2012

Department of Management Services' Response
To the Auditor Generals' Information Technology Operational Audit of the
Department of Management Services
Division of Retirement
Integrated Retirement Information System (IRIS)

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.

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.

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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin, CPA
Page 3
November 15, 2012

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.

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.

Finding No. 4: Security Controls – User Authentication

Certain security controls related to user authentication needed improvement.

Recommendation:

The Department should improve user authentication controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response:

The Division of Retirement concurs with this recommendation. The Auditor General reported 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 recommendations.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

David W. Martin, CPA
Page 4
November 15, 2012

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 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.

The written configuration management plan will reflect the changes above. This will be completed by March 31, 2013.