



AUDITOR GENERAL

DAVID W. MARTIN, CPA



DEPARTMENT OF MANAGEMENT SERVICES

DIVISION OF RETIREMENT

INTEGRATED RETIREMENT INFORMATION SYSTEM (IRIS)

Information Technology Audit

SUMMARY

Pursuant to Section 121.1905, Florida Statutes, the mission of the Department of Management Services (Department), Division of Retirement (Division) is to provide quality and cost-effective retirement services to members participating in the Florida Retirement System (FRS). The Division 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 selected information technology (IT) functions applicable to IRIS during the period September 2007 through January 2008, with selected actions taken from July 1, 2006, and determining the status of corrective actions regarding prior audit findings disclosed in audit report No. 2004-143. The Retirement On-line application, an extension of IRIS that uses Internet technology to provide information and services to members, employers, and retirees, was not within the scope of this audit.

The results of our audit are summarized below:

Finding No. 1: The Division's IT controls for ensuring the completeness of data received for processing in IRIS needed improvement.

Finding No. 2: Division security controls over the IRIS application, data, and supporting IT environment needed improvement.

Finding No. 3: The Division's program change controls for IRIS needed improvement.

Finding No. 4: The Division's disaster recovery plans were not current and had not been approved by management.

Finding No. 5: We noted instances where software patches and antivirus updates had not been applied in a timely manner.

BACKGROUND

Division employees use IRIS, which was developed by BearingPoint and implemented in 1999, to support the Division'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 issuance of the retired 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. As of December 31, 2007, IRIS and Retirement On-line serviced approximately 735,000 active members, 273,000 retired members, and more than 900 employers.

In November 2001, IRIS and Retirement On-line support, as well as the Division's day-to-day information technology needs, were outsourced to BearingPoint. BearingPoint is responsible for

providing the Division's IT functions, which include network and application security administration, application programming, and database administration functions, at an annual cost of \$2.8 million.

The Department also contracted with Infinity Software Development, Inc., to provide an Independent Information Security Manager (ISM) whose duties included assisting the Division with the administration of the BearingPoint contract by providing independent monitoring and oversight of BearingPoint's performance in managing the Division's day-to-day IT operations.

Finding No. 1:

Input Controls

Effective IT application controls include input controls to ensure the completeness of data that is received for processing by the system. For input data that is received in batches, input controls include the use of batch control totals, such as record counts that are included with batch input files and programmatically compared to system-calculated totals, to ensure the completeness of the file submitted for processing.

Following each retired payroll, the Department of Financial Services (DFS) sent the Division information on check numbers and EFT payments made through a warrant register file, which contained a count of records within the file. Our audit disclosed that when the file was processed by the Division in IRIS, the record counts were not verified to ensure that all records to be provided by DFS were received and processed. The absence of a record count verification increased the risk that an incomplete warrant register file, should one be submitted, would not be timely detected by the Division.

Recommendation: The Division should implement controls to ensure that the total number of records sent by DFS in the warrant register file are actually processed in IRIS by verifying control totals.

Finding No. 2: Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that the Division's management of security over the IRIS application, data, and supporting IT resources needed improvement, as described below:

- The Division had one security administrator and one backup security administrator for the IRIS application security software. The primary and backup security administrators shared a single administrator account and password. As a result of the shared account, it was not possible for the Division to distinguish which individual performed security administration functions within the security software.
- The application security software did not have a logging function available. Because there was no logging of the activities performed in the security software, there was no method to determine when changes to security groups, security roles, or individual user access rights were implemented. The lack of a logging function also prevented management from reviewing access modifications made within the security software.
- Effective IT controls include a segregation of duties whereby IT staff are restricted from having update access privileges to production data, except in emergency or unusual situations where access may be granted on a temporary basis. We noted that IT support staff working on IRIS had update access privileges in IRIS, which were inconsistent with a proper segregation of duties. Specifically, a network administrator had complete access privileges in IRIS by being granted all production IRIS roles. Also, the project manager and two developers had the IRIS production role of Calculations 1, which provided complete access to the Calculations functionality and Calculations Administrative functionality within IRIS. Additionally, another developer had the production role of Investment Plan 0, which provided complete access to the investment plan workflow functionality within IRIS. Each of the roles allowed ongoing update access privileges in

IRIS. By allowing IT staff update capability within IRIS, the risk is increased that unauthorized or erroneous disclosure, modification, or destruction of information will occur and not be timely detected.

- Department Policy Number 9.08 provided that a user's access authorization be immediately removed from the system when the user's employment was terminated or the user transferred to a position where access privileges to the system were no longer required. Our review of network access privileges of 29 Division employees, BearingPoint staff, subcontractors, and interns listed as terminated between July 1, 2006, and September 30, 2007, disclosed that network access privileges for two terminated Division employees were not timely removed. One employee, who terminated on October 10, 2007, retained her network access privileges for 14 days, until the date of audit inquiry, October 24, 2007. The other employee, who terminated on October 26, 2006, retained her network access privileges for at least 18 days after her termination date, as she had logged on to the network on November 13, 2006. Additionally, the Division was unable to determine what activities this terminated employee performed while logged in after her termination date. Without timely removal of the access privileges of terminated employees, the risk is increased that the access privileges could be misused by the former employees or others.
- Periodic reviews of the appropriateness of network access privileges were not performed by the ISM or other designated individuals. Without periodic reviews of network access privileges, the risk is increased that inappropriate or unnecessary access privileges will not be timely detected and corrected.
- The Division established accounts on its external file transfer protocol (FTP) server for State and local government agencies to use in transmitting member data to the Division by FTP. Of the 1,230 agency FTP accounts established on the Division's server as of January 10, 2008, only 41 were being actively used by agencies to transmit data to the Division. The Division had not contacted the agencies associated with the unused FTP accounts to determine if the FTP privileges were still necessary or could be removed. The

untimely removal of unused user accounts increases the risk that an unauthorized individual may use the access privileges to read, modify, or delete sensitive information or cause erroneous or unauthorized transactions to be processed.

- Privileges for physical access to the Division's IT facilities were not always promptly removed for persons who no longer needed access. The Division used an employee notification form as a means to request that an individual's access to Division facilities be removed. However, two BearingPoint employees who stopped working on the Division's contract on January 2, 2007, and September 13, 2007, respectively, were still listed on an access list, dated January 25, 2008, as having access privileges to the Division's facilities. The Division could not provide an employee notification form for one employee upon audit request and procedures were not properly followed for the other employee. The Division also could not provide evidence that the former BearingPoint employees' facility access cards were recovered or destroyed. In response to audit inquiry, the Division, on January 25, 2008, deleted the individuals' access privileges to the Division's facilities. Without prompt removal of access privileges upon termination or reassignment, the risk is increased that former or reassigned employees or others will inappropriately gain access to Division IT facilities and misuse IT equipment and the data and software contained therein.
- Certain Division security controls relating to the protection of backup files, management of access privileges, monitoring of security events, management of software patches, and configuration of database and operating system software, in addition to the matters discussed above, needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising Division information security. However, appropriate Division personnel have been notified of these issues. Without adequate security controls, the integrity, confidentiality, and availability of data and IT resources may be compromised, increasing the risk that Division data and IT resources may be subject to improper disclosure, destruction, or modification.

Recommendation: The Division should strengthen its IT security controls in the areas described above to provide increased assurance of the confidentiality, integrity, and availability of the IRIS application, data, and supporting IT resources. The Division should also consider utilizing the expertise of the contracted ISM to assist in monitoring the appropriateness of BearingPoint staff's access privileges.

Finding No. 3:

Program Change Controls

Effective program change controls include provisions for a group independent of the application programmers to control the movement of programs from the test environment to the production environment. It is also good business practice for program changes to be documented, reviewed, and approved. The likelihood of program change controls being followed on a consistent basis as intended by management is increased when management's expectations are clearly communicated to IT personnel in the form of written policies, procedures, and other guidelines.

Our audit disclosed the following aspects of the Division's program change controls applicable to IRIS that needed improvement:

- PL/SQL is a programming language used to manipulate IRIS data in the Oracle database. New or modified IRIS PL/SQL objects (programs) initiated by System Investigation Report (SIR) or Technology Support Center (TSC) requests were developed and moved into production by the same BearingPoint development staff.
- Of 29 IRIS program changes tested, 2 lacked sufficient documentation of user testing and acceptance. In addition, 3 IRIS changes lacked documentation identifying what changes were made and who moved the changes into production.
- The BearingPoint Capability Maturity Model (Software Development Plan) in effect and provided to us on September 14, 2007, was dated April 24, 2003. The Plan was used to update the IRIS application in response to user issues, additional user required

functionality, and special projects identified by management. Information regarding BearingPoint project staff, included in the Plan's organization chart and job descriptions, did not reflect the BearingPoint team in place at the time of audit inquiry. Additionally, the description and flowchart of the change request processes did not document the roles of SIR coordinators or the SIR steering committee. In response to audit inquiry, BearingPoint staff updated the Software Development Plan (dated October 27, 2007).

- The process for checking out, developing, documenting, testing, and checking in application code was described in Build Procedure Instructions. However, the revised Software Development Plan, dated October 27, 2007, did not include a reference to the Build Procedure Instructions. Furthermore, neither document included procedures describing how developers were to check-out, develop, document, test, and check-in PL/SQL programs.
- The Division did not have written database administration policies or procedures covering Division specific areas such as patch management, controlling database access, and setting database security parameters. Database administrators instead relied on vendor-provided documentation, such as user, administrator, and developer guides to perform administrative duties, such as creating tablespaces, creating primary objects, monitoring and optimizing performance, and backing up and restoring the database. The vendor-provided documentation contained generic operational guidelines rather than guidelines that were specific for the IRIS operational environment.

When the program change process is not adequately controlled, the risk is increased that unauthorized or erroneous programs will be moved into the production environment and not be timely detected. Without established current change control policies and procedures, the risk is increased that staff will not consistently perform the program change control duties as expected by management.

Recommendation: The Division should implement controls to establish an appropriate segregation of duties with regard to PL/SQL changes and ensure that appropriate change control documentation is maintained. In addition, the Division, supported by BearingPoint IT services, should develop, update, and periodically review change control policies and procedures to provide increased assurance that procedures remain current.

**Finding No. 4:
Disaster Recovery Plans**

Disaster recovery plans are intended to facilitate a timely and orderly resumption of critical operations in the event of a disaster or other interruption in service. To be most effective, disaster recovery plans should reflect the current operating environment and be approved by key stakeholders, such as senior management, data center management, and program managers.

Department Policy Number 9.10 required staff to maintain disaster recovery plans and follow a designated schedule of testing and updating the plans. However, the Division of Retirement Disaster Recovery Plan, dated May 10, 2007, and the Division of Retirement IT Disaster Recovery Plan, dated June 23, 2006, were not up to date. For example, the Plans did not reflect the relocation of IRIS in April 2006 to a different data center. In addition, neither Plan included evidence of approval by Division management.

Without current and approved disaster recovery plans, the risk is increased that the Division will not resume its IT-dependent business processes in a timely and orderly manner should an interruption in IT services occur.

Recommendation: The Division, supported by BearingPoint IT services, should update and periodically review disaster recovery plans to provide increased assurance that continuity-of-operation provisions remain appropriate.

**Finding No. 5:
Software Patches and Updates**

Patch management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within software by employing a systematic, accountable, and documented process for the timely identification, testing, and application of software patches.

Department Policy Number 9.04 provides that Unix administrators have one week to apply operating system patches or provide written justification to supervisors, managers, and the Office of Information Security. As of October 8, 2007, the Division's operating system vendor was aware of two vulnerabilities within the operating system and had released patches that remedied the two vulnerabilities. However, the patches had not been installed as of November 29, 2007, contrary to the one-week installation requirement defined in Department policy. In addition, documentation was not available justifying the delay, also contrary to the policy. IT support staff indicated that the delay of the deployment of the patches was due to the implementation of a Storage Area Network device on November 5, 2007, but could not provide documentation of the implementation process. In response to audit inquiry, Division staff indicated that the operating system patches were subsequently installed on December 2, 2007.

The Division's management of patches and updates to database and antivirus software also needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising Division information security. However, appropriate Division personnel have been notified of these issues.

Without a proactive, systematic, and documented patch management practice, patches may not be installed in a timely manner, increasing the risk that IT vulnerabilities will persist and be exploited, jeopardizing IT security.

Recommendation: The Division should strengthen its software patch management practices and ensure compliance with appropriate Department policies.

PRIOR AUDIT FINDINGS

Finding Nos. 2 through 4 above included issues repeated from our audit report No. 2004-143. Other IT deficiencies noted in the prior audit have been corrected or were in the process of being corrected.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls related to IRIS and to determine whether the Division had corrected, or was in the process of correcting, deficiencies disclosed in audit report No. 2004-143.

The scope of our audit focused on evaluating selected IT controls applicable to IRIS during the period September 2007 through January 2008, with selected actions taken from July 1, 2006. The Retirement On-line application was not within the scope of our audit.

This IT audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. In conducting our audit, we interviewed appropriate Division personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to IRIS.

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 information technology audit.



David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated April 16, 2008, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

This audit was conducted by Earl Butler, CISA, and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850-488-0840).

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.myflorida.com/audgen/>); by telephone (850-487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

APPENDIX A
MANAGEMENT RESPONSE



Office of the Secretary
4050 Esplanade Way
Tallahassee, Florida 32399-0950
Tel: 850.488.2786
Fax: 850.922.6149
www.dms.MyFlorida.com

Governor Charlie Crist

Secretary Linda H. South

April 16, 2008

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 your tentative and preliminary findings and recommendations contained in the draft report.

If further information is needed concerning our response, please contact Steve Rumph, Inspector General, at 488-5285.

Sincerely,

A handwritten signature in blue ink, appearing to read 'L. South', is written over a horizontal line.

Linda H. South
Secretary

Attachment

cc: David Faulkenberry, Deputy Secretary

Mr. David W. Martin
April 16, 2008
Attachment Page 1

**Department of Management Services' Response
To the Auditor General's Information Technology Audit of
*Department of Management Services
Division of Retirement
Integrated Retirement Information System (IRIS)***

Finding No. 1: Input Controls

The Division's IT controls for ensuring the completeness of data received for processing in IRIS needed improvement.

Recommendation:

The Division should implement controls to ensure that the total number of records sent by DFS in the warrant register file are actually processed in IRIS by verifying control totals.

Response:

A System Investigation Request (SIR) based on this finding was submitted. The SIR requested a control total verification to ensure that the total number of records sent to the Division by DFS was processed when the warrant file is updated in IRIS. The anticipated completion date for this SIR is April 30, 2008.

Finding No. 2: Security Controls

Division security controls over the IRIS application, data, and supporting IT environment needed improvement.

Recommendation:

The Division should strengthen its IT security controls in the areas described above to provide increased assurance of the confidentiality, integrity, and availability of the IRIS application, data, and supporting IT resources. The Division should also consider utilizing the expertise of the contracted ISM to assist in monitoring the appropriateness of BearingPoint staff's access privileges.

Response:

The Division has implemented or will implement the following security controls to strengthen the confidentiality, integrity, and availability of IRIS:

Mr. David W. Martin
April 16, 2008
Attachment Page 2

- The Division is no longer sharing an administrator account to administer application security in IRIS. Each security administrator has their own account and the former shared account was deactivated. This was completed on March 31, 2008.
- The Division will implement an “activity date/time” and “activity user id” trigger on the security database tables that will allow for the tracking of updates to the security profiles. This is a standard in IRIS and was not implemented in the original security schema. This enhancement will be implemented by May 31, 2008.
- The Division will revoke all production roles from IT personnel and assign the generic inquiry role that is available in IRIS. This will be completed by April 30, 2008
- 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 satisfactory manner notifying IT Services of terminated employees. This sets into motion a wide range of activities including removing security access to IRIS and the Divisions physical facilities. This practice extends to non-employees, including BearingPoint. In the two cases cited in the audit, the work process failed to identify terminated employees. More emphasis will be placed on supervisors adhering to the requirement that they complete the necessary forms when employees terminate. An additional notification practice was added on March 25, 2008 to help catch any terminated employees missed by this work process. Whenever a personnel action request (PAR) terminating an employee is created, the supervisor will also send an e-mail to IT Services informing them of the termination. Although the Division could not determine what all activities were performed by the terminated user, the Division is able to review the activity logs and determine that the person did not access the IRIS application.
- The Division will update its procedure to include a review of active network accounts on the same semi-annual basis currently used for appropriate IRIS access. The anticipated effective date of this procedure is June 30, 2008.
- The Division has reviewed the established accounts on its external FTP server and removed accounts that are no longer active. This was completed on March 31, 2008. The Division will update its procedure to review active external FTP accounts on a semi-annual basis. The procedure will be updated by June 30, 2008.
- The Division will also utilize the expertise of the contracted ISM to assist in monitoring BearingPoint staff’s access privileges. This procedure should be in place by June 30, 2008.

Mr. David W. Martin
April 16, 2008
Attachment Page 3

Finding No. 3: Program Change Controls

The Division's program change controls for IRIS needed improvement.

Recommendation:

The Division should implement controls to establish an appropriate segregation of duties with regard to PL/SQL changes and ensure that appropriate change control documentation is maintained. In addition, the Division, supported by BearingPoint IT services, should develop, update, and periodically review change control policies and procedures to provide increased assurance that procedures remain current.

Response:

The Division and BearingPoint has implemented or will implement the following changes to the change control procedures for IRIS:

- BearingPoint will update the change control policy with regards to migration of PL/SQL programs. Only members of the Database Administrator group will be able to migrate PL/SQL programs from test into production. Furthermore, should a Database Administrator (DBA), which also functions as a developer, make a change that needs migration, another member of the DBA group will migrate the change into production. This change will be effective by May 31, 2008.
- BearingPoint and the Division have instituted process improvements to the SIR Management process to increase accountability and improve documentation. The process now includes identifying system updates made and who migrated the updates into production. Furthermore, end user acceptance and sign-off are now mandatory prior to updates migrating into production. This process improvement was completed on February 15, 2008.
- BearingPoint will enhance the software development plan to include software development procedures for SIRs that only affect PL/SQL programs. This will be completed by May 31, 2008.
- BearingPoint will create a set of operational procedures that are specific to maintaining the IRIS database. The documentation will be used in conjunction with Oracle Operations Manuals and will include items that are specific to our installation of Oracle. This will be completed by July 31, 2008.

Finding No. 4: Disaster Recovery Plans

The Division's disaster recovery plans were not current and had not been approved by management.

Mr. David W. Martin
April 16, 2008
Attachment Page 4

Recommendation:

The Division, supported by BearingPoint IT services, should update and periodically review disaster recovery plans to provide increased assurance that continuity-of-operation provisions remain appropriate.

Response:

In addition to reviewing and updating the Divisions Disaster Recovery Plan once a year, the Division will implement a procedure to obtain signatures from the Division Director and Department CIO to serve as final signoff of the updated plan. Final signoff of the updated Disaster Recovery Plan is expected to be received by April 30, 2008.

Finding No. 5: Software Patches and Updates

We noted instances where software patches and antivirus updates had not been applied in a timely manner.

Recommendation:

The Division should strengthen its software patch management practices and ensure compliance with appropriate Department policies.

Response:

The Division is currently implementing the appropriate controls to ensure compliance with the Department's policies.