DEPARTMENT OF MANAGEMENT Services

Office of Inspector General
Department of Management Services
4040 Esplanade Way, Suite 135
Tallahassee, Florida 32399-0001
Tel: 850.488.5285
Fax: 850.921.3066
www.dms.MyFlorida.com

Governor Charlie Crist

Secretary Linda H. South

MEMORANDUM

DATE: October 17, 2008

TO: Linda H. South, Secretary

FROM: Steve Rumph, Inspector General

SUBJECT: **Six-Month Status Report to Auditor General Report No. 2008-172**

Pursuant to Section 20.055(5)(g), Florida Statutes, the following is our explanation of the six-month status of findings and recommendations included in the Auditor General's Report No. 2008-172, ***Department of Management Services, Division of Retirement, Integrated Retirement Information System (IRIS)***. Our response addresses the findings and recommendations in the same order as they appear in the report.

Six-Month Status Report

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.

Original 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.

Current Status of Recommendation:

BearingPoint has completed the control total verification SIR and it was placed in production on May 13, 2008. There have been 26 weekly or monthly payrolls processed since the edit was implemented May 13, 2008, and the counts have matched correctly each time with a message in the Batch Log saying that the RP240 and RP260 files match.

OIG Position

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

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.

Original Response:

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

A. 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.

B. 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.

C. 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.

D. 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.

E. 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.

F. 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.

G. 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.

Current Status of Recommendation:

A. Previously completed.

B. BearingPoint implemented a trigger for "Activity date/time" and "Activity user id" on the security database tables on May 29, 2008. Samples of the updated columns were verified by the ISM.

C. IRIS Production roles removed, replaced with inquiry only role for IT personnel. This change was completed on April 30, 2008 and was verified by the ISM.

D. The previous ISM had validated the additional notification practice that is currently in place and functioning. Additionally, when a new ISM is in place they will develop and implement a quarterly procedure to audit this procedure as follows:

A complete list of Employee Notifications by quarter is received from Administrative Services. Up to 10 records are randomly selected for review. Documentation concerning the final disposition of these records is requested from the Technical Service Center (TSC). The documentation is reviewed for compliance with the policy.

The Division of Retirement is currently in the process of awarding a new contract for the services of an ISM. A contract deliverable will be included in the contract which requires the ISM to develop a procedures manual which incorporates a quarterly review process of Employee Notifications to assure compliance with the policy. It is anticipated that the procedures manual will be completed by June 30, 2009.

E. BearingPoint updated the procedure for reviewing active network accounts and completed the semi-annual review on June 30, 2008. The account review was verified by the ISM.

F. BearingPoint updated the procedure for reviewing active external FTP accounts and completed the semi-annual review on June 30, 2008. The account review was verified by the ISM.

G. The new ISM will develop a quarterly procedure to review not only BearingPoint staff privileges, but several other procedures as well:

1. Validation that Employee Notifications sent to the TSC have been properly completed.
2. Compliance with the Review Procedure for Active Network Accounts.
3. Compliance with the Review Procedure for External FTP Accounts.
4. Compliance with the Security Procedure for Violations regarding Quarterly Health Checks.
5. Compliance with the Review Procedure for Database User Accounts. Compliance with Departmental and Divisional Patch Management Procedures.

The Division of Retirement is currently in the process of awarding a new contract for the services of an ISM. A contract deliverable will be included in the contract which requires the ISM to develop a procedures manual which incorporates a quarterly review process of the above procedure to ensure compliance with the policy. It is anticipated that the procedures manual will be completed by June 30, 2009.

OIG Position

We agree that the Division has implemented security controls to strengthen the confidentiality, integrity, and availability of IRIS, However, we recommend that this finding remain open until the ISM has developed a procedures manual that incorporates the above mentioned procedures in items D and G.

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.

Original Response:

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

A. 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.

B. 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.

C. 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.

D. 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.

Current Status of Recommendation:

A: BearingPoint has updated the Change Control Policy (Configuration Management Plan). PL/SQL changes are now migrated by the DBA group. Furthermore if a DBA changes PL/SQL as a developer, a different DBA migrates the changes to production. Configuration Management Plan changes were verified by the ISM.

B: Previously completed.

C: BearingPoint has updated the Software Development Plan for SIRs that affect PL/SQL programs. The Software Development Plan was verified by the ISM.

D: BearingPoint has written up Operational Procedures for some tasks specific to our installation. These are used in addition to Oracle's published documentation, and help us with very specific tasks so the DBA team can follow consistent procedures. The Operational Procedures were verified by the ISM.

OIG Position

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

Finding No. 4: Disaster Recovery Plans

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

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.

Original 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.

Current Status of Recommendation:

BearingPoint and the Division completed its review and update of the Disaster Recovery Plan. The plan has been signed by both the Division Director and Department CIO (See Attachment – Division Disaster Recovery.pdf).

OIG Position

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

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.

Original Response:

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

Current Status of Recommendation:

BearingPoint continues to work with the Department to strengthen its patch and update procedures. BearingPoint will work with the new ISM to develop a

process to review the patches that have been applied versus what's available on its major applications. BearingPoint will continue to work with the Department and adhere to industry standard for applying patches and updates.

The Division of Retirement is currently in the process of awarding a new contract for the services of an ISM. A contract deliverable will be included in the contract which requires the ISM to develop a procedures manual which incorporates a process for performing reviews to ensure that patches have been applied which are available on its major applications. It is anticipated that the procedures manual will be completed by June 30, 2009.

OIG Position

We agree that the actions taken by the Division should resolve the issue. However, we recommend that this finding remain open until a formal procedures manual is developed which includes a process for reviewing patches that have been applied versus what is available on its major applications.

If further information is needed, please contact John Davis, Auditor Director, or myself at 488-5285.

JSR/gz

cc: Terry L. Shoffstall, Director
Joint Legislative Auditing Committee

David W. Martin, Auditor General

Ken Granger, Chief of Staff
Department of Management Services

David Faulkenberry, Deputy Secretary
Department of Management Services

Sarabeth Snuggs, Director, Division of Retirement
Department of Management Services