REPORT NO. 2009-200
APRIL 2009

DEPARTMENT OF MANAGEMENT SERVICES

DIVISION OF RETIREMENT
INTEGRATED RETIREMENT INFORMATION SYSTEM (IRIS)

Follow-Up on Prior Audit Findings

Information Technology Operational Audit

December 2008 Through February 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF MANAGEMENT SERVICES

Pursuant to Section 20.22(1), Florida Statutes, the Secretary of the Department of Management Services (DMS) is appointed by the Governor, subject to confirmation by the Senate. Linda H. South served as Secretary during the audit period.

The audit team leader was Earl Butler, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by 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 at www.myflorida.com/audgen; by telephone at (850) 487-9024; 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)

Follow-Up on Prior Audit Findings

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 determining the Department's corrective actions regarding prior audit findings relating to IRIS that were disclosed in our report No. 2008-172. Our audit included the period December 2008 through February 2009.

The results of our follow-up audit are summarized below:

Finding No. 1: The Division improved its IT controls for ensuring the completeness of data received for processing in IRIS by implementing the use of control totals to verify the completeness of Department of Financial Services retiree payroll information.

Finding No. 2: The Division addressed many of the security control issues from the prior audit. However, improvements were still needed in the areas of logging changes to access privileges and authenticating the identity of file transfer protocol (FTP) server users.

Finding No. 3: The Division addressed most of the program change control issues from the prior audit. However, its Software Development Plan still needed updating to accurately reflect the current roles and identity of BearingPoint staff.

Finding No. 4: The Technology Support Center (TSC) Disaster Recovery Plan needed updating to reflect current staffing and current backup procedures.

Finding No. 5: Department policy needed updating to reflect current Division operating system security patch procedures.

BACKGROUND

The Division uses IRIS 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 the issuance of the retiree payroll file that is processed by the Department of Financial Services (DFS). IRIS is also used to process and maintain FRS Investment Plan payrolls and data. The Retirement On-line application is an extension of IRIS that uses Internet technology to provide information and services to members, employers, and retirees.

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. The Department also contracted with KPMG 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.

FINDINGS AND RECOMMENDATIONS

Our prior audit disclosed that IRIS controls needed improvement in five areas: input controls, security controls, program change controls, disaster recovery plans, and software patches and updates. This follow-up audit disclosed that the Department had made progress in improving most IRIS controls in the identified areas, but some issues remained unresolved. Specifically, of the five findings disclosed in the prior audit, the Department had corrected one and partially corrected four. Details of the status of the Department's corrective actions relating to the prior audit findings as of February 2009 are disclosed in Table 1.

Definitions of Prior Audit Finding Status

- **Corrected:** Successful development and use of a process, system, policy, or control to correct a prior audit finding.
- **Partially Corrected:** A process, system, policy, or control to correct a prior audit finding was not completely developed or was successfully developed but was not consistently or completely used.
- **Not Corrected:** Preliminary analyses have been performed for correcting the prior audit finding, but the finding has not yet been corrected.

Table 1: STATUS OF PRIOR AUDIT FINDINGS NOTED IN AUDIT REPORT NO. 2008-172 AS OF FEBRUARY 2009

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
			Finding No. 1: Input Controls	
1	N/A	Following each retiree payroll, the DFS sent the Division information on check numbers and electronic funds transfer (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.	**Corrected:** The Division implemented procedures to use control totals to verify that the records intended to be provided by DFS were received and processed by the Division.	N/A
			Finding No. 2: Security Controls	
2	1	The primary and backup IRIS security administrators shared a single administrator account and password.	**Corrected:** The Division's primary and backup IRIS security administrators were assigned unique administrator accounts. In addition, the shared administrator account was disabled.	N/A
2	2	The IRIS 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.	**Partially Corrected:** The Division applied triggers to the security database tables to record which security administrator made a change to an account and when. However, a log was not maintained of specific changes made to a user's IRIS access privileges.	The Division should implement a logging mechanism to record specific changes made to a user's IRIS access privileges.
2	3	IRIS IT support staff had update access privileges in IRIS that were inconsistent with a proper separation of duties.	**Corrected:** IRIS IT support staff have now been assigned the ViewOnly role that does not grant update access privileges.	N/A

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
2	4	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. Additionally, the Division was unable to determine what activities one terminated employee performed while logged in after her termination date.	**Corrected:** A Network User ID Listing, as of December 18, 2008, showed all terminated employee network accounts as disabled and not subsequently used. In addition, the Division determined how to identify subsequent activity on network accounts, should the activity occur.	N/A
2	5	Periodic reviews of the appropriateness of network access privileges were not performed by the ISM or other designated individuals.	**Corrected:** The Division now performs a review of active network accounts on a semi-annual basis. In addition, the Division's independent ISM performs reviews of compliance with security procedures for active network accounts and database user accounts.	N/A
2	6	The Division established accounts on its external 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.	**Corrected:** The Division is now using a new FTP server that has accounts for only those agencies that are still submitting files to the server. The unused agency accounts that had been set up on the previous FTP server were removed prior to the implementation of the new server. In addition, the Division now periodically reviews accounts to determine whether the accounts are still being used.	N/A
2	7	Privileges for physical access to the Division's IT facilities were not always promptly removed for persons who no longer needed access.	**Corrected:** The listing of individuals with physical access to the Division's IT facilities included only persons who needed access to the facilities.	N/A
2	8	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 needed improvement.	**Partially Corrected:** The Division had corrected most of the identified security control issues. However, the Division still needed to improve the authentication of FTP server users. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Division management of the specific issue.	The Division should enhance the authentication of FTP server users.

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
			Finding No. 3: Program Change Controls	
3	1	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.	**Corrected:** The Bearing Point development staff has now been restricted from moving programs into production.	N/A
3	2	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.	**Corrected:** For the items tested during the current audit, program changes were documented appropriately.	N/A
3	3	The BearingPoint Capability Maturity Model (Software Development Plan) in effect and provided to us on September 14, 2007, was dated April 24, 2003. 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.	**Partially Corrected:** The Software Development Plan, dated March 13, 2008, and provided to us on December 24, 2008, did not document the roles of some BearingPoint project staff and had not been updated to reflect changes in BearingPoint project staff that had occurred.	The Division should timely update the Software Development Plan to accurately reflect the current roles and staffing of BearingPoint.
3	4	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.	**Corrected:** The Software Development Plan, Configuration Management Plan, and the Build Procedure Instructions have been updated to collectively provide procedures for PL/SQL program change control.	N/A

Finding No.	Bullet No.	Prior Audit Report Finding Issue	Condition Noted in Current Audit	Current Recommendation
3	5	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.	**Corrected:** The Division developed database administration policies and procedures reflecting the IRIS operational environment.	N/A
			Finding No. 4: Disaster Recovery Plans	
4		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.	**Partially Corrected:** Although now approved by Division management, the TSC Disaster Recovery Plan, dated March 30, 2008, and provided to us by the Division on December 24, 2008, had not been updated to reflect current staff or current backup operating procedures. Updates to the Division of Retirement Disaster Recovery Plan, dated May 10, 2007, are no longer required because the Division Plan was replaced by the TSC Disaster Recovery Plan.	The Division should update the TSC Disaster Recovery Plan to reflect current staffing and operating procedures.
			Finding No. 5: Software Patches and Updates	
5		Operating system patches had not been installed, contrary to the one-week installation requirement defined in Department policy. In addition, documentation was not available justifying the delay, also contrary to policy. The Division's management of patches and updates to database and antivirus software also needed improvement.	**Partially Corrected:** The Division has migrated to a different operating system and now maintains its operating system security through the application of current security patches provided by the vendor. In addition, the application of patches and updates to database and antivirus software was improved. However, Department policy had not been updated to address security patches for the Division's new operating system environment.	The Department should update its policy to address the Division's new operating system environment.

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 in accordance with applicable 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 whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2008-172.

The scope of our audit, which was for the period December 2008 through February 2009, focused on evaluating the Department's corrective actions regarding IT control deficiencies applicable to IRIS disclosed in the prior audit.

In conducting our audit, we:

- Interviewed appropriate personnel at the Division.
- Obtained an understanding of applicable Department and Division procedures in the areas of input controls, security controls, program change controls, disaster recovery plans, and software patches and updates.
- Observed, documented, and tested the effectiveness of selected Department and Division input controls, security controls, program change controls, disaster recovery plans, and software patches and updates.

AUTHORITY

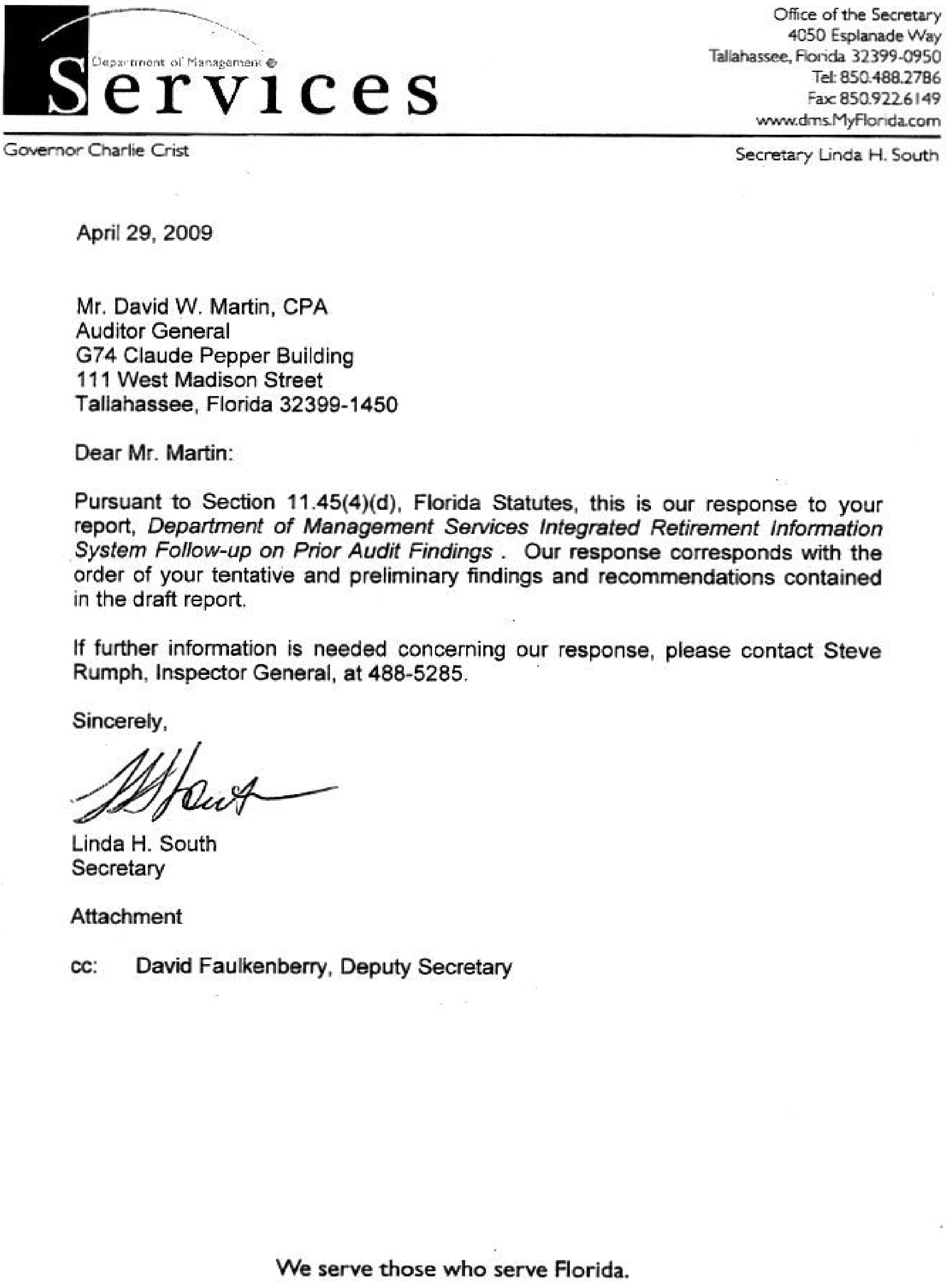
Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated April 29, 2009, 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



Department of Management Services

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 29, 2009

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 Follow-up on Prior Audit Findings* . 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,

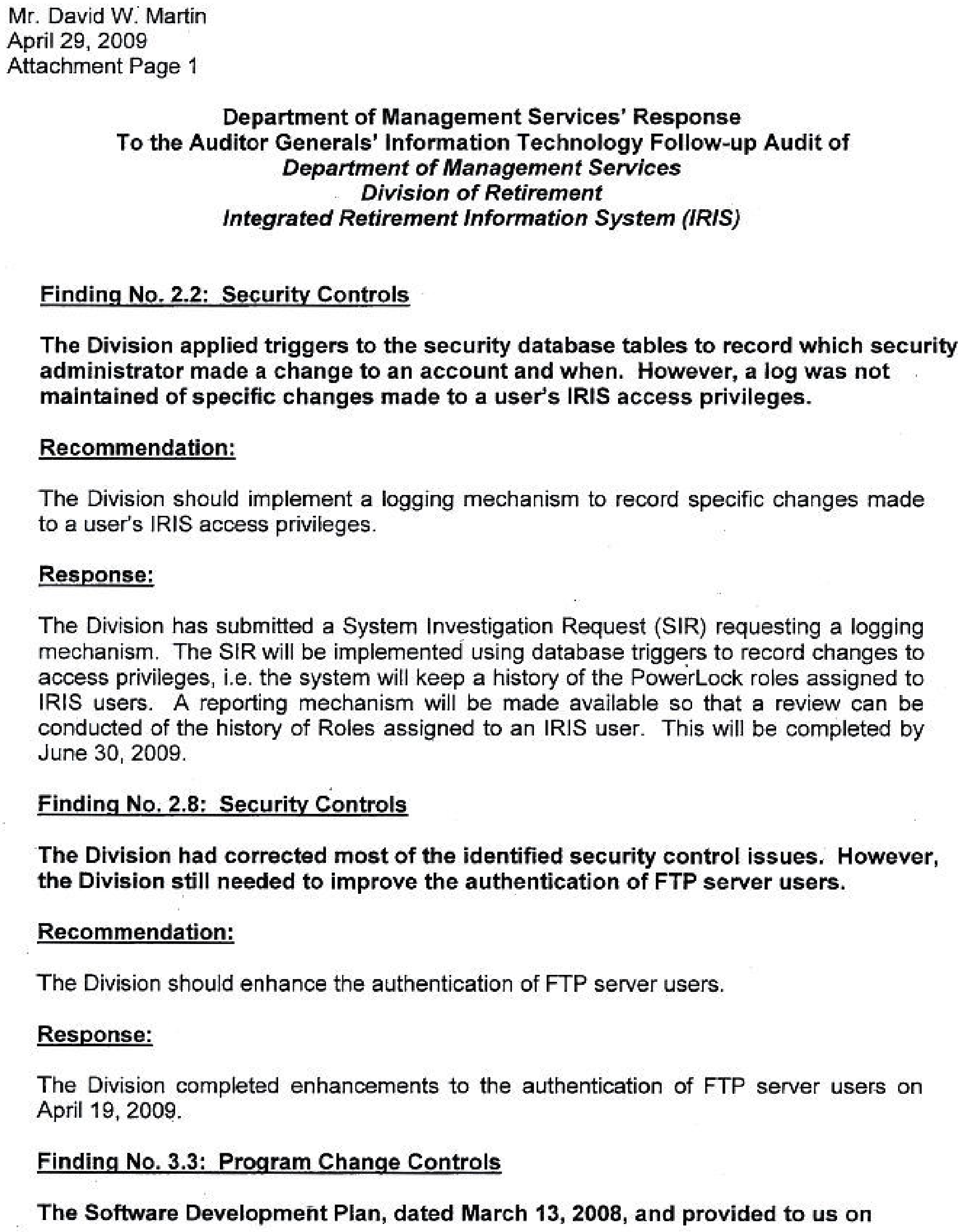
Linda H. South
Secretary

Attachment

cc: David Faulkenberry, Deputy Secretary

We serve those who serve Florida.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE



Mr. David W. Martin
April 29, 2009
Attachment Page 1

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

<u>Finding No. 2.2: Security Controls</u>

The Division applied triggers to the security database tables to record which security administrator made a change to an account and when. However, a log was not maintained of specific changes made to a user's IRIS access privileges.

<u>Recommendation:</u>

The Division should implement a logging mechanism to record specific changes made to a user's IRIS access privileges.

<u>Response:</u>

The Division has submitted a System Investigation Request (SIR) requesting a logging mechanism. The SIR will be implemented using database triggers to record changes to access privileges, i.e. the system will keep a history of the PowerLock roles assigned to IRIS users. A reporting mechanism will be made available so that a review can be conducted of the history of Roles assigned to an IRIS user. This will be completed by June 30, 2009.

<u>Finding No. 2.8: Security Controls</u>

The Division had corrected most of the identified security control issues. However, the Division still needed to improve the authentication of FTP server users.

<u>Recommendation:</u>

The Division should enhance the authentication of FTP server users.

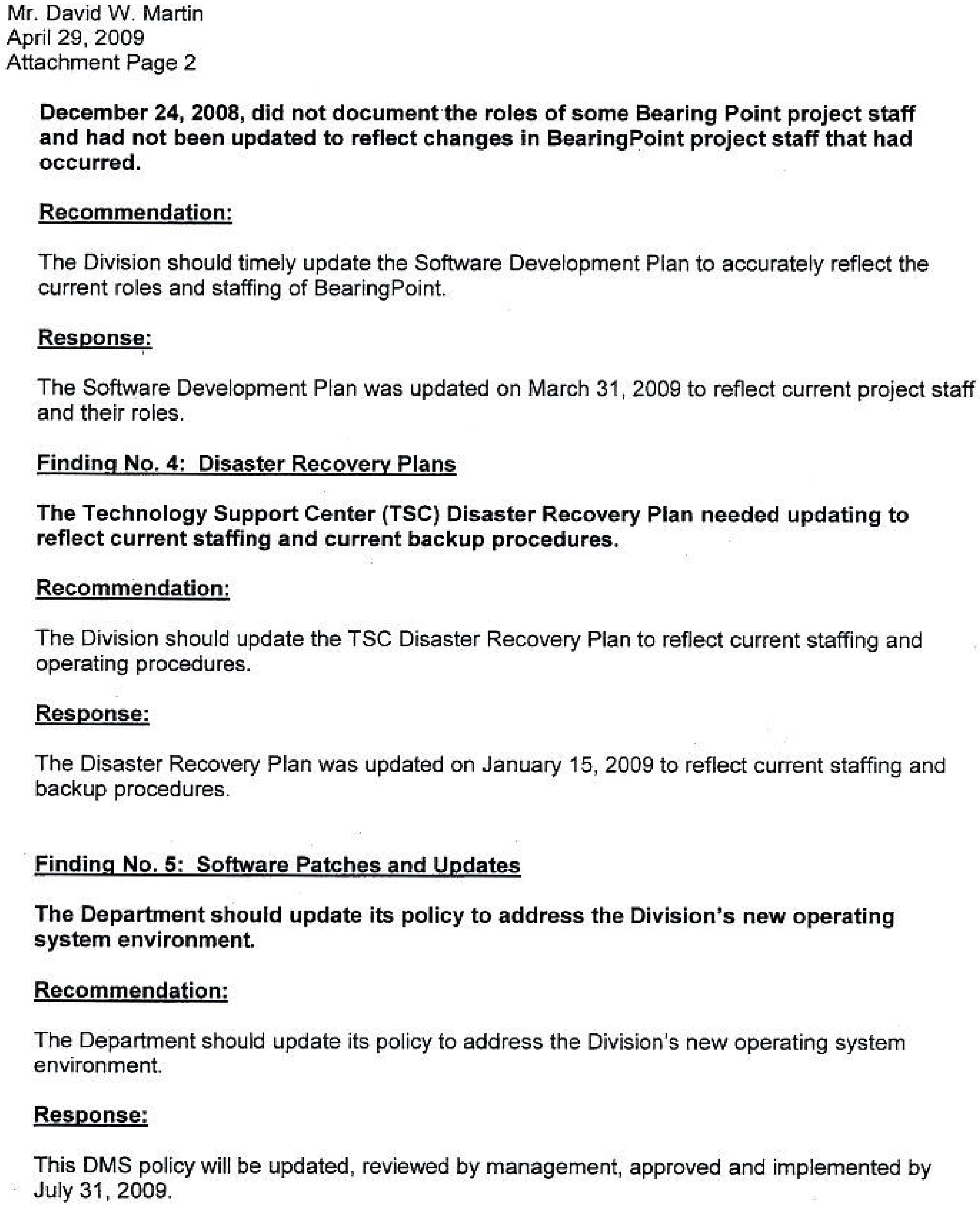
<u>Response:</u>

The Division completed enhancements to the authentication of FTP server users on April 19, 2009.

<u>Finding No. 3.3: Program Change Controls</u>

The Software Development Plan, dated March 13, 2008, and provided to us on

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE



Mr. David W. Martin
April 29, 2009
Attachment Page 2

December 24, 2008, did not document the roles of some Bearing Point project staff and had not been updated to reflect changes in BearingPoint project staff that had occurred.

Recommendation:

The Division should timely update the Software Development Plan to accurately reflect the current roles and staffing of BearingPoint.

Response:

The Software Development Plan was updated on March 31, 2009 to reflect current project staff and their roles.

Finding No. 4: Disaster Recovery Plans

The Technology Support Center (TSC) Disaster Recovery Plan needed updating to reflect current staffing and current backup procedures.

Recommendation:

The Division should update the TSC Disaster Recovery Plan to reflect current staffing and operating procedures.

Response:

The Disaster Recovery Plan was updated on January 15, 2009 to reflect current staffing and backup procedures.

Finding No. 5: Software Patches and Updates

The Department should update its policy to address the Division's new operating system environment.

Recommendation:

The Department should update its policy to address the Division's new operating system environment.

Response:

This DMS policy will be updated, reviewed by management, approved and implemented by July 31, 2009.