



STATE OF MISSISSIPPI
HALEY REEVES BARBOUR, GOVERNOR
DEPARTMENT OF HUMAN SERVICES
DON THOMPSON
EXECUTIVE DIRECTOR

January 12, 2010

Mr. Stacey Pickering, State Auditor
Office of the State Auditor
State of Mississippi
P.O. Box 956
Jackson, Mississippi 39205

Dear Mr. Pickering:

The information contained in this letter addresses the audit findings identified by the Office of the State Auditor (OSA) during the 2009, Information Technology Security Audit conducted for the Mississippi Department of Human Services (MDHS).

We appreciate the State Auditor and EDP Audit Staff for the professional manner in which the audit was conducted and the supportive attitude of the auditors participating in this project.

1. **Finding: MDHS Should Improve Its Legacy Application Security -**

Response: We concur with the audit finding and support the recommendation to make application security a top priority for all of our legacy applications.

Corrective Action Plan: MIS has a number of security projects, some underway while others are pending approval with funding needed to go forward. Because the legacy applications are over 15 years old and have been customized or enhanced numerous times, there are basically three options:

- a.) Convert the application to a newer, more modern technology like Java and DB2. Make enhanced security part of the design requirements whether in-house developed or vendor package. If chosen, all division directors would be needed to support and co-fund this decision by March 31, 2010.
- b.) Design and develop a new security interface, mandatory for all applications to utilize for access authorization. If chosen, all division directors would be needed to support and co-fund this decision by March 31, 2010.

- c.) Reassign the application security functions to another team within MIS and tighten restrictions on who has authority to request and make changes. MIS Director would make this decision By March 31, 2010.

Recommendation: Option "b" is the best action plan due to its universal solution to the access security concerns for all applications on the MDHS network. However, because "b" requires monetary funding, option "c" is the best immediate "stop-gap" solution.

2. ***Finding: Back-up Files for In-house Servers Should Be Stored Offsite (Recurring finding)***

Response: We concur with the audit finding and its recurrence. We also agree with the audit recommendation to do something, even if it's a short, "stop-gap" solution. The recurrence of this finding has much to do with the two issues below:

- a.) delays with implementation of the server virtualization solution underway at MDHS and ITS
- b.) costs allocation of the expense associated with the technical expertise needed to modify the IBM "Tivoli" system being used daily for the MDHS server backups

Corrective Action Plan:

- a.) ITS must give MDHS an updated conversion date for virtualization by January 31, 2010.
- b.) ITS must give MDHS a firm date and costs associated with their move to the new data center on Lakeland Drive by February 28, 2010.
- c.) MIS will perform a risk analysis for applications affected by the server backups not going offsite by March 31, 2010.
- d.) Based on the answers to "a","b" and "c" above, MIS will make a decision to wait or move forward with a MDAH solution. MIS will make this decision by April 15, 2010.
- e.) If the decision is made to move forward with the MDAH direction, this process will be implemented by MIS no later than June 30, 2010.

3. ***Finding: MDHS Should Document Its Natural Database Policies and Procedures -***

Response: We concur with the audit finding.

Corrective Action Plan:

MDHS MIS will be developing security and change control standards by December 31, 2010, which will be new for the server side and rewritten for the mainframe process. Also, all standards, policies and procedures will be documented, kept up to date and digitally stored on the document imaging database by the MIS area.

Mr. Pickering
January 12, 2010
Page three

4. **Finding: MDHS Should Assign a Coordinator For Its IT Disaster Contingency Plan -**
Response: We concur with the audit finding and the recommendation.
Corrective Action Plan: MDHS MIS will be developing a Disaster Recovery Open Issues List by June 30, 2010, which will carry over from each test to the next. MIS will assign a technical resource from Computer Operations to monitor the annual "live" test and expedite problem solutions as they occur. Any issues remaining unresolved at the end of the test window coming up in August 2010, will be assigned to the appropriate area and resolution made before the next DR test in 2011.

5. **Finding: MDHS Should Formalize A Policy for Computer Room Access -**
Response: We concur with the audit finding and the recommendation.
Corrective Action Plan: MDHS cleaned up the current access report the same day the discrepancies were brought to the attention of MIS and has since implemented a semi-annual review committee meeting to analyze who has access, to where and update accordingly. This review committee will meet before June 30, 2010 and again before December 31, 2010. We have also tightened up the timeframe between HR and MIS Security, for the removal of employee access authority (physical and online) when we have retirements, terminations, resignations, etc. Also, temporary access for consultants, contractors and vendors is revoked as soon as their work is done.

6. **Finding: MDHS Should Reduce Excessive LAN Administrator Rights -**
Response: We concur with the audit finding and the recommendation.
Corrective Action Plan: MIS will enforce this restriction by having a quarterly review to determine who has or should not have LAN Administrator authority, who needs or should have LAN Administration authority and then make changes accordingly. As a result, we are developing for rollout by March 31, 2010 documentation which will outline the level of authority and responsibility for a LAN Administrator. Additionally, at the same time, MIS will include the documented duties and responsibilities for the Server Administrator and Database Administrator.

If there are any questions or if you need additional information, please contact Tim Ragland, Director, MDHS Division of MIS, at 601-359-4600 or tim.ragland@mdhs.ms.gov.

Sincerely,



Don Thompson
Executive Director

DT:TR:lb