



STATE OF MISSISSIPPI
HALEY REEVES BARBOUR, GOVERNOR
DEPARTMENT OF HUMAN SERVICES
DONALD R. TAYLOR
EXECUTIVE DIRECTOR

August 8, 2007

Mr. Phil Bryant
Office of the State Auditor
P.O. Box 956
Jackson, MS 39205

Dear Mr. Bryant:

The information contained in this correspondence is in response to your letter dated July 17, 2007, pertaining to the limited assessment of the Electronic Data Processing (EDP) general controls and selected application controls for the Mississippi Department of Human Services (MDHS), that was initiated on March 27, 2007, and completed on May 11, 2007.

I have reviewed the documentation you provided regarding the immaterial control deficiencies involving electronic data processing that require attention by MDHS management. MDHS has enclosed documentation that represents our response to the audit findings and outlines our plan to implement required changes and enhancements to our control processes to ensure we are in compliance with certain regulations and industry best practices.

I appreciate the cooperation and courtesy extended by your staff: Toby Frazier, CISA, Mike Ferguson and LaDonna Johnson, throughout this assessment. If you have questions or need more information, please contact me.

For a better Mississippi,


Donald R. Taylor

Enclosure as stated

DRT:WTD:mab

**Mississippi Department of Human Services
Division of Management Information Systems**

Responses to EDP General Controls Audit

August 8, 2007

IMMATERIAL CONTROL DEFICIENCIES

1. In-house Servers Back-up Files Should Be Stored Offsite

Finding:

MDHS is currently using an automated system to perform daily back-ups of Windows 2003 servers, but the back-ups are not being stored off-site. MDHS MIS informed us that they were in the process of implementing an off-site storage plan. Failure to maintain system back-ups off-site could result in the loss of all LAN data and slow any recovery efforts in the event of an on-site disaster.

Recommendation:

We recommend that all MDHS servers back-up files should be stored offsite. This process should be documented in the MIS Disaster Plan.

MDHS Response:

The MDHS MIS Division has initiated the process to identify the best method for implementing Offsite Storage by communicating with the Department of Information Technology Services (ITS) effective August 7, 2007. In this communication, MDHS is asking for recommendations from ITS on utilizing services they may be able to provide for this need rather than MDHS procuring services from a Network Integration Vendor to implement an offsite storage solution.

In addition to discussing Offsite Storage in this communication with ITS, MDHS included a description of our need for support in developing a Disaster Recovery Plan for the Servers and Network infrastructure located at the MDHS State Office. MDHS intends to aggressively pursue identification of requirements to implement Offsite Storage and to implement the solution as soon as possible.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Mike Bullard.
- C. Projected Completion Date - March 2008.

2. MDHS Should Provide For Regular Network Reviews

Finding:

MDHS last had a network review conducted in June 2005. As a result of this review, a remediation plan was created to resolve the issues noted in the review. Management indicated that currently, there are no plans in the budget to fund another network review. Regular network reviews are an important tool in maintaining and strengthening the critical infrastructure of a telecommunications network.

Recommendations:

We recommend that MDHS establish a scheduled network review program.

MDHS Response:

The MDHS Agency concurs with the Auditor's comments regarding the benefits associated with periodic network reviews and remediation. MDHS appreciates the special funding that the Office of the State Auditor provided in 2005, for all State Agencies to conduct a Network review. In addition to conducting that required network review, the MDHS Agency has conducted the following additional network reviews to strengthen the security of MDHS networks.

- Fall 2006 - Pileum Corporation conducted a comprehensive review of MDHS network systems. Pileum and the MDHS Network staff created a priority list for remediation steps so that needed changes could be made to enhance network security for the Agency. The budgeted hours available in this engagement were not sufficient to complete all of the tasks identified. Funding for this engagement was provided by the Office of the State Auditor based on a request submitted from the MDHS MIS Division.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

● Spring 2007 - Pileum Corporation continued remediation work to make changes to the MDHS network to strengthen security. The priority list for remediation work was updated. The final summary report of all Pileum audit and remediation work is scheduled to be delivered to MDHS in August 2007. That report will outline the additional work to be addressed in the next engagement which is planned for Spring 2008.

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Mike Bullard.
- C. Projected Completion Date - March 2008.

3. MDHS Should Improve Documentation of Server and Desktop Systems Patch Management Process

Finding:

MDHS is performing patch management on their Windows 2003 servers, but there appears to be a lack of documentation to support this function. It is important to document patch management administration activities to insure that critical updates have been evaluated and applied.

Recommendation:

We recommend that MDHS develop and implement a formal plan for documenting the patch management process.

Response:

Following this audit process, the MDHS MIS Network group implemented the Windows Software Update Services (WSUS) application, with assistance from Pileum. WSUS is a software tool created by Microsoft that enables the User to automate the Patch Management process. MDHS is now using WSUS for Patch Management of MDHS Servers. The WSUS application, which is available from Microsoft at no cost, provides documentation of software Patches that have been applied and any exceptions that exist. We believe with the implementation of WSUS, MDHS will consistently meet or exceed Server Patch Management guidelines.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Mike Bullard.
- C. Projected Completion Date - Completed.

4. MDHS Should Better Control Powerful RACF Emergency Fix ID's Provided to Programming Staff

Finding:

We noted that a RACF generic ID provided to a programmer for use in "after hours" emergencies to correct production problems was used for normal program changes. This circumvented the normal change control process.

Routine use of powerful emergency user-ID's violates separation of duties principles and CobiT DS 5.3 Identity Management: "Access should be defined in line with documented business needs". Bypassing the formal change control process may allow unapproved programs to be placed into production.

Upon the results of EDP Audit's review, MDHS MIS Department canceled the RACF generic ID.

Recommendation:

We recommend that MDHS develop a procedure to insure the RACF generic ID's provided to correct production problems after hours are being used in the manner intended. Review of any powerful RACF User-ID's should be part of the regular MIS self-audit procedures.

MDHS Response:

As the Auditor noted, the MDHS MIS Division immediately disabled two RACF generic IDs once it was brought to our attention that these were still in use during normal business hours. This was a carry over from special support that was required during the Katrina recovery process. The MDHS MIS Security group will ensure that these special RACF IDs are restricted to "On Call" use only.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Mike Bullard.
- C. Projected Completion Date - Completed.

5. MDHS Should Reassess User Access Rights on a Periodic Basis

Finding:

From our review of RACF user authorities, certain MDHS computer operations staff was noted to have unneeded access to MVS LOADLIBS. At one time, computer operations required this access to perform duties of moving programs from test into production. The program change process now utilizes a separate computer programmer to move programs into production. Unnecessary authority of access to production program libraries can create an exposure for unauthorized program changes.

CobIT DS 5.4, User Account Management, requires that computer access authority should be limited to only what an individual needs to perform his job: "Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. Perform regular management review of all accounts and related privileges."

Recommendation:

We recommend that MDHS reassess RACF access rights in relation to access needs of users on a periodic basis to insure job duties have not changed, and that rights to access files and datasets are still valid based on such assessments.

MDHS Response:

MDHS MIS did make the necessary system access changes to the computer operations staff as soon as this information was provided to us by the State Audit staff.

MDHS will develop procedures to validate all Users that have RACF access. This will require that MDHS validate access for over 3,000 employees located in over 100 locations. We believe this validation process will be a valuable systems security tool to ensure all inactive Users have been deleted from MDHS systems and that existing Users have the appropriate level of access.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Mike Bullard.
- C. Projected Completion Date - March 2008.

6. The MDHS MIS Disaster Contingency Plan Should be Updated

Finding:

We reviewed the MDHS MIS Disaster Recovery Plan Manual as part of our audit procedures. We found the manual was outdated, as several of the key personnel listed are no longer employed by the agency.

Regular maintenance of the IT Continuity Plan is recommended by CobiT DS 4.4" "Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. It is essential that changes in procedures and responsibilities be communicated clearly and in a timely manner." Failure to maintain an up to date Disaster Recovery Plan Manual could impede the department's ability to timely recover operations in the event of a disaster.

Recommendation:

We recommend that MDHS MIS update its Disaster Recovery Plan Manual. Additionally, we recommend that this manual be reviewed to assure that the provisions outlined coordinate and compliment with the newly written MDHS COOP (Continuity of Operations Plan) document.

MDHS Response:

The MDHS MIS Division will perform a re-write and complete update of the Disaster Recovery Manual. The updated manual will be integrated, where appropriate, with the new Continuity of Operations Plan (COOP). An annual review and update of the MDHS MIS Disaster Recovery Manual will be scheduled and conducted.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Mike Bullard.
- C. Projected Completion Date - March 2008.

7. The MAVERICS and MVS Applications Program Change Management Process Should Be Improved

Finding:

The EDP Audit Section chose the MAVERICS system for an application change control process review, as it is a significant MDHS application system. Part of the objectives of a program change review on MVS mainframes include steps to verify that only authorized programs are executing and that a quality control process is evidenced to stakeholder review and acceptance of any program changes.

To test program change control procedures, we identified any MAVERICS programs which had been changed within the last 18 months. We then compared the documentation on file of the change to the change control process outlined for MAVERICS in the MDHS MIS "Standards and Procedures Manual." We selected a random sample of 12 program change control documentation folders from 110 indicated program changes in our 18 month selection period from the MAVERICS application in MDHS MIS.

Three of the twelve sampled program change documentation folders could not be located. We also that in a significant portion of the folders sampled, the documentation inside the folders was often variable and was not complete enough to reflect the entire change process and, in some cases did not contain a sign-off of acceptance for quality control purposes.

Overall, we found the change control process as outlined in the MDHS MIS "Standards and Procedures Manual" to meet acceptable standards for a program change control process. However, we noted that the program change control process employed are segmented by application, rather than a standard department wide methodology for change management on MVS applications.

**Mississippi Department of Human Services
Division of Management Information Systems
Responses to EDP General Controls Audit**

Control of program changes may not be as effective as it could be due to the lack of a true change management system. For example, as noted in our finding number four (4), one programmer may have been using an emergency fix RACF ID to bypass the formal change control process.

Recommendation:

We recommend that MDHS MIS review the program change documentation folders and incorporate any changes to forms and procedures that are appropriate to ensure that all program change steps are recorded per the "Standards and Procedures Manual," including noting quality control acceptance and appropriate check-off that notification of branch offices of the program change was made. Procedures should be reviewed to help ensure that all program change folders are complete and accounted for. Evaluation of other methods for program change management may prove beneficial to MDHS.

MDHS Response:

Based on this Audit process and recommendations, the MDHS MIS Division has made changes to the "Service Request Completion Checklist" to ensure that all of the required documentation has been completed for all program changes. A signature field has been added to the "Service Request Completion Checklist" to ensure that the stakeholder reviews and accepts the change and acknowledges that the change satisfies the request specifications originally provided. The stakeholder will notify the branch offices of changes that will impact their workflow.

The issue regarding the use of an emergency fix RACF ID is addressed above in article 4, and documents that issue has been resolved.

Correction Action Plan:

- A. Specific Steps - The steps to be taken are included in the response section.
- B. Contact Person - Brenda Wilson.
- C. Projected Completion Date - September 2007.

MDHS would like to thank the State Audit staff for their "partnership approach" while working with the MDHS MIS Division during this audit process. The positive relationship developed between the State Audit staff and the MDHS MIS Division will enable these entities to work together on an on-going basis to ensure that all steps possible are taken to ensure a high level of security is maintained for MDHS computer systems.