



STATE OF MISSISSIPPI
OFFICE OF THE STATE AUDITOR
STACEY E. PICKERING
STATE AUDITOR

October 2, 2008

Information Systems Management Report

Don Thompson, Executive Director
Mississippi Department of Human Services
P. O. Box 352
Jackson, MS 39205

Dear Mr. Thompson:

The Office of the State Auditor has completed its limited assessment of the Information Systems (IS) general controls and selected application controls of the Mississippi Department of Human Services, as of July 3, 2008. This assessment was performed in conjunction with the audit of the State of Mississippi. The Office of the State Auditor's staff members participating in this IS review engagement included: Toby Frazier, CISA, Mike Ferguson CISA, and LaDonna Johnson.

The fieldwork for these assessment procedures was begun on June 2, 2008. These procedures cannot and do not provide absolute assurance that all state legal requirements have been met. In accordance with Section 7-7-211, Miss. Code Ann. (1972), the Office of the State Auditor, when deemed necessary, may conduct additional procedures for this or other fiscal years to ensure compliance with legal requirements.

In planning and performing our limited assessment of the MDHS IS general controls, we considered the Mississippi Department of Human Service's internal control over electronic data processing in order to determine our assessment procedures but not for the purpose of expressing an opinion on the effectiveness of the internal control over electronic data processing. These procedures were performed primarily through observations and discussions with Mississippi Department of Human Services' Management Information Systems Department personnel and limited testing of selected information in the MAVERICS application system.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

Our consideration of the internal control over electronic data processing was for the limited purpose described in the third paragraph and would not necessarily identify all deficiencies in internal control over electronic data processing that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in the internal control over electronic data processing and its operation that we consider to be a material weakness, as defined above.

However, we noted certain immaterial weaknesses in internal control over electronic data processing that require the attention of management. These matters are noted under the heading IMMATERIAL WEAKNESSES IN INTERNAL CONTROL. As part of obtaining reasonable assurance about whether selected IS general controls of the Mississippi Department of Human Services were functioning as designed, we performed assessments of compliance with certain regulations and industry best practices. However, providing an opinion on compliance with those regulations and practices was not an objective of our assessment and, accordingly, we do not express such an opinion.

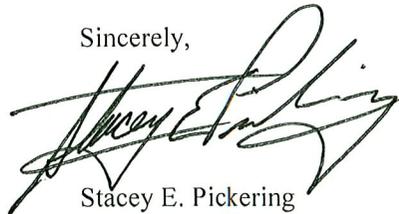
Please review the recommendations included in this report and submit a plan to implement them by, October 23, 2008. The enclosed findings contain more information about our recommendations.

During future engagements, we may review the findings in this management report to ensure procedures have been initiated to address these findings.

This report is intended solely for the information and use of management and Members of the Legislature and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties. However this report is a matter of public record and its distribution is not limited.

I appreciate the cooperation and courtesy extended by the officials and employees of the Mississippi Department of Human Services throughout this assessment. If you have any questions or need more information, please contact me.

Sincerely,



Stacey E. Pickering
State Auditor

Enclosures

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF HUMAN SERVICES
AS OF JULY 3, 2008**

TABLE OF CONTENTS

	Page No.
I. ABBREVIATIONS USED IN THIS REPORT	4
II. REVIEW OBJECTIVES AND APPROACH	5
III. STANDARD OF BEST PRACTICES	5
IV. FINDINGS AND RECOMMENDATIONS	6
<u>IMMATERIAL WEAKNESSES IN INTERNAL CONTROL</u>	
Finding 1. Back-up Files for In-house Servers Should Be Stored Offsite	6
Finding 2. MDHS Should Improve Its Network Review and Remediation Process.....	6
Finding 3. MDHS Should Improve Its RACF Security Self-Audit Process.....	7
Finding 4. MDHS Should Improve Its LAN Self-Audit Process.....	7
Finding 5. MDHS Should Better Control Powerful RACF Emergency Fix User-IDs.....	8

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF HUMAN SERVICES
AS OF JULY 3, 2008**

I. ABBREVIATIONS USED IN THIS REPORT

DOS	Disk Operating System (Microsoft 1980's)
EBT	Electronic Benefits Transfer
FITS	Financial Information Tracking System
IS	Information Systems
IT	Information Technology
ITS	Mississippi Department of Information Technology Services
LAN	Local Area Network
MAVERICS	Mississippi Applications Reporting Information and Control System
MDHS	Mississippi Department of Human Services
MIS	Management Information Systems
MVS	IBM Mainframe: Multiple Virtual Storage
OSA	Office of the State Auditor
RACF	Resource Access Control Facility (IBM)
RFP	Request for Proposals
TANF	Temporary Assistance for Needy Families
WAN	Wide Area Network

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF HUMAN SERVICES
AS OF JULY 3, 2008**

II. REVIEW OBJECTIVES AND APPROACH

Our review's overall objective was to perform an assessment of the general data processing controls established by management of the Mississippi Department of Human Services (MDHS) to support the integrity and security of the financial information processed by the computer systems of the MDHS at its main office in Jackson, Mississippi. To accomplish these objectives, the Information Systems Audit Section staff of the Office of the State Auditor (OSA) performed the following:

- Met with MDHS management and the OSA financial auditors to gain an understanding of the critical MDHS processes and controls;
- Interviewed selected MDHS technology and management personnel;
- Reviewed available documentation of procedures, standards and other evidential matter;
- Performed audit tests to verify the existence and effectiveness of the processes and controls in place to meet the objectives delineated above; and
- Identified any vulnerabilities associated with any weaknesses, if noted, in the control environment.

Our approach was not designed to specifically detect illegalities, fraudulent acts, errors or other irregularities.

III. STANDARD OF BEST PRACTICES

In this report we will refer to best practices standards that should be achieved by all Information Technology (IT) departments, specifically we mention and endorse the methodology of CobIT 4.0 of the IT Governance Institute (www.itgi.org) as the industry standard we have selected for the evaluation of the IT control environment. Other similar methodology is the Information Technology Infrastructure Library (ITIL) which is a framework of best practice approaches intended to facilitate the delivery of high quality IT services. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both quality and value for money in IT operations. These procedures are supplier independent and have been developed to provide guidance across the breadth of IT infrastructure, development, and operations.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF HUMAN SERVICES
AS OF JULY 3, 2008**

IV. FINDINGS AND RECOMMENDATIONS

IMMATERIAL WEAKNESSES IN INTERNAL CONTROL

1. Back-up Files for In-house Servers 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. This exception was noted in our prior year's audit and remediation is planned but as of our review date had not been implemented. MDHS MIS informed us that they were still 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.

2. MDHS Should Improve Its Network Review and Remediation Process

Finding:

A network vulnerabilities review was conducted for MDHS in June of 2005 by a private contractor. As a result of this review, a remediation process contract was started during 2006 for identified higher risk vulnerabilities. Upon completion of these services in 2007, the private contractor issued a status report which identified network vulnerability mitigation actions had been taken, and what actions still should be taken by MDHS.

Our procedures determined that while MDHS MIS has remediated the higher risk vulnerabilities noted in the 2005 network review report, some server patches had not been applied. MDHS MIS did not create any documentation indicating internal acknowledgement of the outstanding issues, or plans for further remediation, beyond the 2006 remediation contract.

Maintaining complete documentation on identified vulnerabilities and completion of mitigation efforts is an important role in security management. Without a process of documentation of vulnerabilities and actions taken to keep systems up to date, risks may exist where significant security vulnerabilities could be overlooked.

CobIT DS5.5 states that IT security implementation should be tested and monitored proactively and should be reaccredited periodically to insure the approved security level is maintained.

Recommendation:

We recommend that MDHS establish a scheduled network review program. We also recommend that MDHS establish a program that will provide for a reasonable network security evaluation process on an ongoing basis to track changes that need to be made and accomplishments achieved.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF HUMAN SERVICES
AS OF JULY 3, 2008**

3. MDHS Should Improve Its RACF Security Self-Audit Process

Finding:

MDHS has an ongoing program of reviewing RACF to insure its user base is current. However, we noted that the RACF users should also have their access rights periodically re-evaluated to insure privileges granted are appropriate to current job duties.

CobiT DS5.5 states that IT security implementation should be tested and monitored proactively and should be reaccredited periodically to insure the approved security level is maintained.

Recommendation:

We recommend that MDHS develop and implement a proactive security evaluation plan which would include periodic RACF user reaccreditation. The reaccreditation process could be done on a rotating basis per year insuring the entire RACF user population is reviewed in a reasonable timeframe.

4. MDHS Should Improve Its LAN Self-Audit Process

Finding:

MDHS manages the local building LAN using Novell, and also maintains nearly 3,000 users in an active directory via Windows Server 2003. During our 2007 review, MDHS was evaluating a security management tool to assist with proactive security management of the active directory users; however a toolset was not acquired. While a purchase of any toolsets to assist in management of an active directory environment would be very useful, it may not be a mandatory item for effective management of the Windows Server 2003 environment. Scripts may be written and run which can provide important management information.

At the time of our review, MDHS had not implemented any process to evaluate its active directory LAN security, other than just baseline control settings. It appeared that the network security group was expecting the acquisition of a toolset and had not developed a fallback plan in the event the toolset was not acquired.

With a large user base such as MDHS, a proactive management process of the active directory is an important security consideration.

Recommendation:

We recommend that MDHS develop and implement a proactive security evaluation plan that would include a comprehensive LAN users and security management process.

**OFFICE OF THE STATE AUDITOR
INFORMATION SYSTEMS MANAGEMENT REPORT
MISSISSIPPI DEPARTMENT OF HUMAN SERVICES
AS OF JULY 3, 2008**

5. MDHS Should Better Control Powerful RACF Emergency Fix User-ID's

Finding:

Last year, we noted that a powerful RACF emergency fix user-ID provided to a programmer for use in “after hours” emergencies had been used for normal program changes which circumvented the normal change control process. Again this year, we found that certain RACF emergency fix user-IDs had been utilized during normal business hours. Although we did not identify any abuse of such IDs, we believe that problems to which fixes are postponed to normal business hours should not require the need of immediate use of powerful emergency fix RACF user-IDs.

Routine use of powerful emergency user-IDs 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.

Recommendation:

Upon notification of the results our review, MDHS MIS Department cancelled all but one of the ID's and created a procedure whereby the use of an emergency fix ID requires logging of the problem requiring such use. Therefore, we recommend that MDHS MIS continue to monitor for any inappropriate use of authorized RACF emergency fix ID's.

End of Report