



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

July 15, 2008

**Information Systems Management Report**

Tommye D. Favre , Executive Director  
Mississippi Department of Employment Security  
P.O. Box 1699  
Jackson, Mississippi 39215-1699

Dear Mrs. Favre:

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 Employment Security as of May 30, 2008. This assessment was performed in conjunction with the federal 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 April 9, 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 IS general controls, we considered the Mississippi Department of Employment Security'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 Employment Security's Information Systems Department personnel and limited testing of information from the Unemployment Insurance Tax 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 and accordingly would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, we believe that none of the deficiencies noted in this report is a material weakness.

We did note certain immaterial weaknesses involving 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 Employment Security 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.

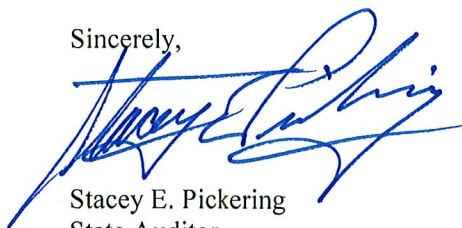
Please review the recommendations included in this report and submit a plan to implement them by August 5, 2008. The enclosed findings contain more information about our recommendations.

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 Employment Security throughout this assessment. If you have any questions or need more information, please contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read "Stacey E. Pickering", is written over a horizontal line.

Stacey E. Pickering  
State Auditor

Enclosures

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY  
AS OF MAY 30, 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>A IMMATERIAL WEAKENSSES IN INTERNAL CONTROL</u>	
Finding 1. MDES Information Systems Department Should Improve Controls for Implementation of Mainframe Application Programs .....	6
Finding 2. MDES Should Periodically Inventory Mainframe Tapes .....	6
Finding 3. MDES Should Limit the Use of the “Special” Attribute in RACF .....	7
Finding 4. MDES Should Remove Terminated Employees from RACF and Active Directory .....	7
Finding 5. MDES Should Test Its Mainframe Computer Disaster Recovery Plan .....	8

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY  
AS OF MAY 30, 2008**

I. ABBREVIATIONS USED IN THIS REPORT

DOS	Disk Operating System (Microsoft 1980's)
FYE	Fiscal Year End
IS	Information Systems
IT	Information Technology
ITS	Mississippi Department of Information Technology Services
LAN	Local Area Network
MDES	Mississippi Department of Employment Security
MVS	Multiple Virtual Storage – IBM Operating System
OSA	Office of the State Auditor
RACF	Resource Access Control Facility (IBM)
RFP	Request for Proposals
UI	Unemployment Insurance (Program)

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY  
AS OF MAY 30, 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 Employment Security (MDES) to support the integrity and security of the financial information processed by the computer systems of the MDES 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):

- Met with MDES IS management and the OSA financial auditors to gain an understanding of the critical MDES processes and controls;
- Interviewed selected MDES technology and accounting 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](http://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 EMPLOYMENT SECURITY  
AS OF MAY 30, 2008**

IV. FINDINGS AND RECOMMENDATIONS

**IMMATERIAL WEAKNESSES IN INTERNAL CONTROL**

1. *Finding:*

MDES Information Systems Department Should Improve Controls for Implementation of Mainframe Application Programs

We noted that mainframe application COBOL programs were placed or compiled and linked into production libraries directly by the application programmer. Best practices as supported by COBIT AI7.8 Promotion to Production states “Implement formal procedures to control the handover of the system from development testing to operations...”

Although there have been few recent changes to the UI Tax system and all appeared to have proper approval, we note that a risk of unauthorized changes to mainframe production programs may exist when a programmer is allowed to move code they wrote or modified into production. This could create the opportunity for unintended results.

*Recommendation:*

We recommend that mainframe application computer programs should be moved into production libraries by staff other than the person who authored that program or modification. In many organizations this task is handled by either the scheduling or computer operations areas.

2. *Finding:*

MDES Should Periodically Inventory Mainframe Tapes

Our inquiry to MDES Information Systems Department’s Computer Operations indicated that they did not maintain an inventory listing of tapes which was verified from time to time.

This practice is supported by the IT Management Goal 14 from COBIT “Account for and Protect all IT Assets.”

Failure to account for all system tapes could present risks of non-detection of any lost tapes which could result in improper disclosures of either employee or employer information, or create issues in critical disaster recovery conditions.

*Recommendation:*

We recommend that the MDES Information Systems Department periodically verify the mainframe tape inventory and document the results of the verification process.

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY  
AS OF MAY 30, 2008**

3. *Finding:*

MDES Should Limit Usage of the RACF “Special” Attribute

The “Special” attribute in RACF, the system which manages MVS security, is a powerful attribute which allows the user full control over RACF. This attribute includes access and modification rights to any resource which is protected by RACF. We found that the “Special” attribute in RACF was granted to 19 individuals at MDES.

COBIT DS5.3 Identity Management states: “... User Access Rights to systems and data should be in line with defined and documented business needs.”

Failure to control or limit the “Special” attribute in RACF may allow individuals to modify or create programs and data without proper authorization.

*Recommendation:*

We recommend that the “Special” RACF attribute be limited to only those people whose job responsibilities require this authority level in the RACF system, or systems programmers which need this authority level to maintain systems services. Certain special RACF attributes such as resetting of passwords may be defined for staff members without giving them the entire “Special” rights authority.

4. *Finding:*

MDES Should Establish a Method to Remove or Isolate Terminated Employees in RACF and Active Directory

Our review of the RACF user population against the MDES 2007 separated employee list indicated that out of 103 employees on that list, 44 were still listed in RACF. Additionally we noted of the 1,223 user-ids in RACF that 163 of these users had not accessed the system since 2006.

We also compared the separated employee list against the MS active directory domain server user-id listing. The active directory domain list controls the MDES internal LAN system and determines who has access authority inside of the LAN and PC’s attached. Our review indicated that 83 separated users or expired user-id’s still existed in active directory.

Our inquiries indicated that MDES Human Resources did not appear to be providing the IT Department with information on employee terminations, therefore the MIS Department was not properly removing these terminated employees in RACF and the active directory.

COBIT DS5.4 User Account Management includes the following best practice statement “Perform regular management review of all accounts and related privileges.”

**OFFICE OF THE STATE AUDITOR  
INFORMATION SYSTEMS MANAGEMENT REPORT  
MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY  
AS OF MAY 30, 2008**

*Recommendation:*

We recommend that MDES document and establish procedures to remove, or isolate terminated employees' user-ids within a short time limit after separation.

5. *Finding:*

MDES Should Test Its Mainframe Computer Disaster Recovery Plan

We conducted a review of the MDES Information Systems Department's mainframe computer disaster recovery plan and related documents. Our work indicated that MDES had contracted with an outside recovery vendor for computer services in case of a disaster. However, MDES has not tested its systems on the offsite vendor's system.

Regular tests insure that systems are compatible and help reduce time required in an actual disaster for recovery of computing services.

Best practices in information technology as supported by COBIT DS4.5 Testing of the IT Continuity Plan suggests "Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered..."

Failure to test recovery plans and systems could result in the non-discovery of system incompatibilities, capacity planning issues, and other information technology driven significant issues.

*Recommendation:*

We recommend that the MDES Information Systems Department conduct testing of the contracted mainframe recovery system at least on an annual basis.

**End of Report**